Ausarbeitung der Vorlesung

Zahlentheorie II

im Wintersemester 2003/04

D. Wolke

1. Kapitel. Das Waringsche Problem

Literatur: Loo–Keng Hua: Introduction to Number Theory (Springer)

Bez. $k \geq 2$; $x, y, x_j, y_j \in \mathbb{Z}$.
$e(\beta) = e^{2\pi i \beta}$.
Die O–Konstanten und die Konstanten C_j hängen höchstens von k ab.

Edmund Waring (1734–1798) vermutete, daß es zu jedem $k \geq 2$ ein natürliches $g(k)$ gibt, so daß sich jedes $n \in \mathbb{N}$ als Summe von höchstens $g(k)$ k–ten Potenzen natürlicher Zahlen schreiben läßt:

$$n = n_1^k + \ldots + n_l^k, \quad 1 \leq l \leq g(k).$$

Im folgenden steht $g(k)$ immer für die kleinstmögliche Anzahl solcher k–ten Potenzen. Für $k = 2$ liefert der Satz von Lagrange den exakten Wert $g(2) = 4$. Allgemein wurde das Problem, in dem Sinn daß $g(k) < \infty$ ist, erst 1909 von Hilbert (David H., 1862–1943) gelöst. Eine Beweisvariante, die sich an die Hilbertsche Methode anschließt, findet man im Buch „Number Theory“ von W. Narkiewicz.

1919 fanden Hardy und Littlewood (Godefrey Harold H., 1877–1947; John Edensor L., 1885–1977) eine Lösung mittels der von ihnen eingeführten **Kreismethode**. Diese läßt sich am Beispiel des Waringschen Problems wie folgt schildern. Sei $N \in \mathbb{N}$,

$$S(\alpha) = \sum_{0 \leq x \leq N^{1/k}} e(\alpha\, x^k),$$

$$R_{k,l}(N) = \#\{(x_1, \ldots, x_l) \in \mathbb{N}_0^l,\ x_1^k + \ldots + x_l^k = N\}.$$

Mit Hilfe der Orthogonalitätsrelation für $e(\beta)$ folgt dann

$$R_{k,l}(N) = \int_0^1 (S(\alpha))^l\ e(-N\alpha)\ d\alpha.$$

Das Integral wird in geeigneter Weise in Teile zerlegt und dort – mit großem technischem Aufwand – asymptotisch ausgewertet. Die Kreismethode liefert bislang die besten Ergebnisse bezüglich $g(k)$. Als Lektüre kann das Buch „The Hardy–Littlewood Method“ von R.C. Vaughan empfohlen werden.

Hier soll eine Methode dargestellt werden, die auf Yuri Vladimiri Linnik (1915–1972; 1943) zurückgeht. Diese wiederum benutzt allgemeine Ergebnisse über Summen von Zahlenmengen (Lew Genrichowitsch Schnirelman, 1905–1938).

1.1. Def. $\mathcal{A}, \mathcal{B} \subseteq \mathbb{N}_0$.

(1) $\mathcal{A} + \mathcal{B} \underset{\text{Df}}{=} \{c \in \mathbb{N}_0,\ \exists\ a \in \mathcal{A}, b \in \mathcal{B} : c = a + b\}$.
„Summe“ der Mengen $\mathcal{A}$ und $\mathcal{B}$.

(2) $n\mathcal{A} \underset{\text{Df}}{=} \{c \in \mathbb{N}_0,\ \exists\ a_1, \ldots, a_n \in \mathcal{A} : c = a_1 + \ldots + a_n\}$.

(3) $\mathcal{A}$ heißt **Basis** (von $\mathbb{N}$), wenn es ein $n \in \mathbb{N}$ gibt mit $n\mathcal{A} \supseteq \mathbb{N}$. Das kleinste solche n heißt die **Ordnung der Basis**.

Das Waring'sche Problem kann hiermit kurz formuliert werden: Ist für jedes $k \geq 2$ die Menge $\mathbb{P}_k \underset{\text{Df}}{=} \{0, 1, 2^k, 3^k, \ldots\}$ Basis von $\mathbb{N}$?

1.2. Def. $\mathcal{A} \subseteq \mathbb{N}_0, n \in \mathbb{N}$.

(1) $A(n) \underset{\text{Df}}{=} \#\{1 \leq a \leq n,\ a \in \mathcal{A}\}$.

(2) $\sigma(\mathcal{A}) \underset{\text{Df}}{=} \inf\limits_{n \in \mathbb{N}} \dfrac{A(n)}{n}$.
Schnirelman–Dichte einer Zahlenmenge. (Man achte darauf, daß inf und nicht lim inf genommen wird).

(3) $\mathcal{A}$ besitzt **positive Dichte**, wenn $\sigma(\mathcal{A}) > 0$ ist.

Folgerungen.

(1) $0 \leq \sigma(\mathcal{A}) \leq 1$.

(2) $\mathcal{A}$ besitzt positive Dichte, gdw. $\exists\ \alpha > 0\ \forall\ n \in \mathbb{N} :\quad A(n) \geq \alpha n$.

(3) $\sigma(\mathcal{A}) = 0$, falls $1 \notin \mathcal{A}$,
$\sigma(\mathcal{A}) \leq \dfrac{n-1}{n}$, falls $n \notin \mathcal{A}$.

1.3. Hilfssatz. $\mathcal{A}, \mathcal{B} \subseteq \mathbb{N}_0,\ 1 \in \mathcal{A},\ 0 \in \mathcal{B}$.
Beh. $\sigma(\mathcal{A}+\mathcal{B}) \geq \sigma(\mathcal{A}) + \sigma(\mathcal{B}) - \sigma(\mathcal{A})\sigma(\mathcal{B})$.
Beweis. Für $n \in \mathbb{N}$ seien $1 = a_1 < a_2 < \ldots < a_r \leq n$ die Elemente von $\mathcal{A} \cap \{1, \ldots, n\}$. Für $1 \leq j \leq r$ werde

$$g_j = a_{j+1} - a_j - 1 \quad (1 \leq j \leq r-1) \quad \text{und} \quad g_r = n - a_r$$

gesetzt. Dann liegen in jedem Intervall $[a_j, a_{j+1})$ bzw. $[a_r, n]$ mindestens $B(g_j)+1$ Elemente von $\mathcal{A}+\mathcal{B}$, nämlich $a_j = a_j + 0$ und $a_j + b_l$ mit $1 \leq b_l \leq g_j$. Man erhält

$$\begin{aligned}(A+B)(n) &\geq r + \sum_{j=1}^{r} B(g_j) \\ &\geq A(n) + \sigma(\mathcal{B}) \sum_{j=1}^{r} g_j = A(n) + \sigma(\mathcal{B})\ (n - A(n)) \\ &\geq n\ \sigma(\mathcal{A})\ (1 - \sigma(\mathcal{B})) + n\ \sigma(\mathcal{B}),\end{aligned}$$

also die Behauptung. □

Der Hilfssatz kann mit erheblichem Aufwand verschärft werden zu

$$0 \in \mathcal{A} \wedge 0 \in \mathcal{B} \Rightarrow \sigma(\mathcal{A}+\mathcal{B}) \geq \min(1, \sigma(\mathcal{A}) + \sigma(\mathcal{B}))$$

(Satz von Mann, 1942).

1.4. Hilfssatz. $0, 1 \in \mathcal{A}$.

Beh. $\sigma(n\mathcal{A}) \geq 1 - (1 - \sigma(\mathcal{A}))^n$.
Beweis durch Induktion. Für $n = 1$ ist nichts zu zeigen. Für $n \geq 1$ ist auf $\mathcal{A}$ und $n\ \mathcal{A}$ Hilfssatz 1.3. anwendbar $(\sigma \underset{\text{Df}}{=} \sigma(\mathcal{A}))$.

$$\begin{aligned}\sigma((n+1)\mathcal{A}) &\geq \sigma + \sigma(n\ \mathcal{A}) - \sigma \cdot \sigma(n\ \mathcal{A}) \\ &\geq \sigma + (1-\sigma)\ (1 - (1-\sigma)^n) \\ &= 1 - (1-\sigma)^{n+1}.\end{aligned}$$

□

1.5. Satz von Schnirelman (1933)
$\mathcal{A} \subseteq \mathbb{N}_0, \quad 0 \in \mathcal{A}, \quad \sigma(\mathcal{A}) > 0$.
Beh. $\mathcal{A}$ ist Basis, d.h. $\exists\ n : n\mathcal{A} = \mathbb{N}_0$
Beweis. Aus $\sigma \underset{\text{Df}}{=} \sigma(\mathcal{A}) > 0$ folgt $1 \in \mathcal{A}$. Nach 1.4. gibt es ein $k \in \mathbb{N}$ mit
$(*) \quad \sigma(k\mathcal{A}) \geq \frac{1}{2}$.

Es wird sich $2k\mathcal{A} = \mathbb{N}_0$ ergeben. Angenommen, es existiert ein $1 < m \in \mathbb{N}$ mit

$$m \notin 2k\mathcal{A} = k\mathcal{A} + k\mathcal{A}.$$

Wegen $0 \in k\mathcal{A}$ folgt daraus $m \notin k\mathcal{A}$.
Nach $(*)$ und Voraussetzung gilt

$$\begin{aligned} m &\leq m(\sigma(k\mathcal{A}) + \sigma(k\mathcal{A})) \\ &\leq (kA)(m) + (kA)(m) = (kA)(m-1) + (kA)(m-1). \end{aligned}$$

Seien $1 = b_1 < \ldots < b_r \leq m-1$ die Elemente von $(k\mathcal{A}) \cap \{1, \ldots, m-1\}$. Wegen $2r \geq m > m-1$ sind $b_1, \ldots, b_r$ und $m-b_1, \ldots, m-b_r$ insgesamt mehr als $m-1$ Zahlen in $[1, m-1]$. Daher existieren $1 \leq j, l \leq r$ mit $b_j = m - b_l$, also $m = b_j + b_l \in 2k\mathcal{A}$, im Widerspruch zur Annahme. □

Für $k \geq 2$ hat die Menge $\mathbb{P}_k = \{0, 1, 2^k, \ldots, \}$ wegen $P_k(m) \leq m^{1/k}$ offenbar die Schnirelman–Dichte Null.

Die Strategie des Linnikschen Beweises zur Waring–Aussage ist wie folgt:

a) Es wird gezeigt, daß es ein $n = n(k)$ gibt mit $\sigma(n\ \mathbb{P}_k) > 0$. Hierin liegt die Hauptschwierigkeit.

b) Mit a) und dem Schnirelmanschen Satz folgt die Behauptung.

Der nächste Hilfssatz dient zum Beweis der entscheidenden Linnikschen Ungleichung 1.7.

1.6. Hilfssatz. Für $a \in \mathbb{Z},\ A, B \geq 1$ sei

$$Q(a) = Q(a, A, B) = \#\{(x_1, x_2, y_1, y_2) \in \mathbb{Z}^4,\ x_1y_1 + x_2y_2 = a,\ |x_j| \leq A,\ |y_j| \leq B\}.$$

Beh.

$$Q(a) \leq \begin{cases} 27A^{3/2}\ B^{3/2}, & \text{falls} \quad a = 0, \\ 60AB \sum\limits_{d|a} \frac{1}{d}, & \text{falls} \quad a \neq 0. \end{cases}$$

Beweis. 1. Fall. $a = 0$. Die x_j und y_j können maximal $2A+1$ bzw. $2B+1$ Werte durchlaufen. Zu einem Tripel (x_1, x_2, y_1) gibt es höchstens ein y_2, so daß $x_1y_1 + x_2y_2 = 0$ erfüllt ist, ebenso bei vorgegebenem (x_1, y_1, y_2). Es gilt daher

$$\begin{aligned} Q(0) &\leq \min((2A+1)^2\ (2B+1),\ (2A+1)\ (2B+1)^2) \\ &\leq 27 \min(A^2B,\ AB^2) \\ &\leq 27(A^2B \cdot AB^2)^{1/2} = 27A^{3/2}\ B^{3/2}. \end{aligned}$$

2. Fall. $a \neq 0,\ A \leq B$. Sei $Q_1(a)$ die Anzahl der Quadrupel (x_1, x_2, y_1, y_2) mit
(1) $\quad x_1y_1 + x_2y_2 = a,\ (x_1, x_2) = 1,\ |x_2| \leq |x_1| \leq A,\ |y_j| \leq B.$
Durch (1) ist $x_1 = 0$ ausgeschlossen.
Für $(x_1, x_2) = 1,\ |x_2| \leq |x_1| \leq A$ sei $Q_2(a, x_1, x_2)$ die Anzahl der Paare (y_1, y_2) mit
(2) $\quad x_1y_1 + x_2y_2 = a, \quad |y_j| \leq B.$

Wegen $(x_1, x_2) = 1$ ist die Gleichung in y_1, y_2 lösbar. Ist (y_{10}, y_{20}) ein festes Lösungspaar, so werden durch

$$y_1 = y_{10} + b\ x_2, \quad y_2 = y_{20} - b\ x_1 \quad (b \in \mathbb{Z})$$

alle anderen Lösungen beschrieben. $|y_1|,\ |y_2| \le B$ ergibt

$$|b| = \Big|\frac{y_{20} - y_2}{x_1}\Big| \le \frac{2B}{|x_1|}.$$

Für b und damit (y_1, y_2) stehen daher wegen $|x_1| \le A \le B$ höchstens

$$2\ \frac{2B}{|x_1|} + 1 \le \frac{5B}{|x_1|}$$

Werte zur Verfügung. Daraus ergibt sich

$$\begin{aligned} Q_1(a) &= \sum_{1 \le |x_1| \le A} \ \sum_{|x_2| \le |x_1|, (x_1, x_2) = 1} Q_2(a, x_1, x_2) \\ &\le \sum_{1 \le |x_1| \le A} \ \sum_{|x_2| \le |x_1|} \frac{5B}{|x_1|} \\ &\le 5B \sum_{1 \le |x_1| \le A} \frac{2|x_1| + 1}{|x_1|} \le 30\ AB. \end{aligned}$$

Läßt man die Bedingung $|x_2| \le |x_1|$ fort, dann verdoppelt sich die Anzahl höchstens, d.h.

(3) $\quad \#\{(x_1, x_2, y_1, y_2),\ (x_1, x_2) = 1,\ x_1 y_1 + x_2 y_2 = a,\ |x_j| \le A,\ |y_j| \le B\} \le 60\ AB.$

Im Fall $(x_1, x_2) = d$ ist die Gleichung äquivalent zu

$$x_1' y_1 + x_2' y_2 = \frac{a}{d}, \quad (x_1', x_2') = 1, \quad |x_j'| \le \frac{A}{d}, \quad |y_j| \le B.$$

Mit (3), das wegen $A/d \le A \le B$ anwendbar ist, folgt

$$Q(a) \le \sum_{d|a} 60\ \frac{A}{d}\ B = 60\ AB \sum_{d|a}\ \frac{1}{d}.$$

3. Fall. $a \ne 0,\ B \le A$. Hier geht man durch Vertauschen der Rollen der x_j und y_j wie im zweiten Fall vor. □

1.7. Hilfssatz (Linnik, 1943).
Sei $A \ge 1, \quad k \ge 2, \quad C_1 \ge 1,$

$$f(x) = a_k\ x^k + a_{k-1}\ x^{k-1} + \ldots + a_1\ x + a_0 \quad \in \mathbb{Z}[x]$$

mit

$$0 < |a_k| \le C_1,\ |a_{k-1}| \le C_1\ A, \ldots, |a_1| \le C_1\ A^{k-1},\ |a_0| \le C_1\ A^k.$$

Sei I ein Teilintervall von $[0, A]$.
Dann gilt

$$J_k = J_k(C_1, A, f, I) \underset{\text{Df}}{=} \int_0^1 \Big| \sum_{x \in I} e\big(f(x)\alpha\big) \Big|^{8^{k-1}} d\alpha = \mathrm{O}(A^{8^{k-1}-k}).$$

Die O–Konstante hängt von C_1 und k ab und kann im Prinzip explizit angegeben werden.

Bemerkungen. 1. Der Beweis wird durch Induktion nach k geführt. Hierzu erweisen sich die eigenwillig erscheinenden Bedingungen an f als günstig. Benutzt wird die Ungleichung schließlich nur für $f(x) = x^k$ und $I = [0, A]$.
2. J_k kann trivial durch $\mathrm{O}(A^{8^{k-1}})$ abgeschätzt werden. Es werden also k A–Potenzen gewonnen. Dies reicht später haarscharf aus.

Beweis des Hilfssatzes.
1. $k = 2$. Hier ist

$$J_k = \sum_{x_1,\dots,x_4,y_1,\dots,y_4 \in I} \int_0^1 e\Big(\big(f(x_1) + f(x_2) - f(y_1) - f(y_2) - f(x_3) - f(x_4) + f(y_3) + f(y_4)\big)\alpha\Big) d\alpha$$

$$\leq \#\big\{(x_1, \dots, x_4, y_1, \dots, y_4),\ 0 \leq x_j, y_j \leq A,$$

$$f(x_1) - f(y_1) + f(x_2) - f(y_2) = f(x_3) - f(y_3) + f(x_4) - f(y_4)\big\} \tag{1.1}$$

Sei

$$x_j' = x_j - y_j, \quad y_j' = a_2(x_j + y_j) + a_1. \tag{1.2}$$

Dann gilt

$$f(x_j) - f(y_j) = a_2(x_j^2 - y_j^2) + a_1(x_j - y_j) = x_j'\ y_j'. \tag{1.3}$$

Aus $0 \leq x_j, y_j \leq A$ folgt nach der Voraussetzung für a_1 und a_2

$$|x_j'| \leq A, \quad |y_j'| \leq 3C_1A. \tag{1.4}$$

Jedem Paar (x_j', y_j') mit (1.4) entspricht nach (1.2) und wegen $a_2 \neq 0$ höchstens ein Paar (x_j, y_j) mit $0 \leq x_j, y_j \leq A$.
Also ist die Anzahl der in (1.1) gezählten 8–Tupel nach (1.3)

$$\leq \#\big\{(x_1', \dots, x_4', y_1', \dots, y_4'),\ |x_j'| \leq A,\ |y_j'| \leq 3C_1A, \quad x_1'y_1' + x_2'y_2' = x_3'y_3' + x_4'y_4'\big\}.$$

Mit Hilfssatz 1.6. und (1.1) ergibt sich

$$J_2 \le \sum_{|a|\le 6C_1A^2} Q^2(a,A,3C_1,A)$$

$$= \mathrm{O}(A^6 + \sum_{0<|a|\le 6C_1A^2} A^4\Big(\sum_{d|a} d^{-1}\Big)^2. \tag{1.5}$$

Die Summe über a ist (mit $B = 6C_1A^2$)

$$\le 2\sum_{m\le B}\ \sum_{d_1|m} \frac{1}{d_1} \sum_{d_2|m} \frac{1}{d_2}$$

$$= 2\sum_{d_1,d_2\le B} \frac{1}{d_1d_2} \sum_{m\le B, m\equiv 0[d_1,d_2]} 1$$

$$\le 2B \sum_{d_1,d_2\le B} \frac{1}{d_1d_2}\,\frac{(d_1,d_2)}{d_1d_2}$$

$$\le 2B \sum_{d_1,d_2\le B} (d_1d_2)^{-3/2} = \mathrm{O}(B) = \mathrm{O}(A^2) \quad \big((d_1,d_2)\le \min(d_1,d_2)\le \sqrt{d_1d_2}\big).$$

Aus (1.5) folgt hiermit

$$J_2 = \mathrm{O}(A^6) = \mathrm{O}(A^{8^{2-1}-2}),$$

wie behauptet.

2. $k > 2$. Die Ungleichung sei für $k-1$ und alle zulässigen Polynome g vom Grad $k-1$ bewiesen. Diese sollen die Voraussetzungen des Hilfssatzes mit einem $C_2 = C_2(C_1,k)$ erfüllen. Alle O–Konstanten hängen nur von C_2 und k, somit allein von C_1 und k ab.

2.1. Sei f ein zulässiges Polynom vom Grad k. Dann gilt für $0 \le \alpha \le 1$

$$\Big|\sum_{x\in I} e(f(x)\alpha)\Big|^2 = \sum_{x,y\in I} e\big(\big(f(y)-f(x)\big)\alpha\big)$$

$$\le A+1+\sum_{0<|b|\le A}\ \sum_{x\in I, x+b\in I} e\big(\big(f(x+b)-f(x)\big)\alpha\big) \tag{2.1.1}$$

$$= A+1+\sum_{0<|b|\le A}\ \sum_{x\in I(b)} e\big(\big(f(x+b)-f(x)\big)\alpha\big).$$

Dabei ist $I(b)$ das durch

$$x\in I \quad \text{und} \quad x+b\in I \tag{2.1.2}$$

festgelegte Intervall.
Für $0 < |b| \le A$ sei

$$
\begin{aligned}
(2.1.3) \qquad g(x) = g(x,b) &= b^{-1}\big(f(x+b) - f(x)\big) \\
&= a_k\ b^{-1}\big((x+b)^k - x^k\big) + \ldots + a_1\ b^{-1}(x+b-x) \\
&= a_k \left(\binom{k}{1} x^{k-1} + \binom{k}{2} x^{k-2} b + \ldots + b^{k-1} \right) + \ldots + a_1 \\
&= \tilde{a}_{k-1} x^{k-1} + \tilde{a}_{k-2}(b) x^{k-2} + \ldots + \tilde{a}_0(b).
\end{aligned}
$$

Man rechnet leicht nach, daß aus den Bedingungen an die a_ν und aus $|b| \le A$

$$
(2.1.4) \qquad \tilde{a}_{k-1} = k\ a_k \neq 0, \quad |\tilde{a}_{k-1}| \le C_2, |\tilde{a}_{k-2}| \le C_2 A, \ldots, |\tilde{a}_0| \le C_2\ A^{k-1}
$$

folgt. $C_2 = C_2(C_1, k)$ wird durch die obigen Ungleichungen festgelegt. Auf die $g(x,b)$ und ihre $I(b)$ wird daher die Induktionsvoraussetzung anwendbar sein.

Setzt man für $0 < |b| \le A$

$$
(2.1.5) \qquad S(b,\alpha) = \sum_{x \in I(b)} e\big(bg(x,b)\alpha\big),
$$

so ergibt sich aus (2.1.1)

$$
(2.1.6) \qquad \Big| \sum_{x \in I} e(f(x)\alpha) \Big|^{2 \cdot 8^{k-2}} \le 2^{8^{k-2}} \max\Big((A+1)^{8^{k-2}}, \ \Big| \sum_{0<|b|\le A} S(b,\alpha) \Big|^{8^{k-2}} \Big).
$$

2.2 Die Höldersche Ungleichung

$$
\Big(\sum \alpha_\nu \beta_\nu \Big)^c \le \Big(\sum \alpha_\nu^{c'} \Big)^{c/c'} \Big(\sum \beta_\nu^c \Big)
$$

$(\alpha_\nu, \beta_\nu \ge 0; \quad c, c' > 0, \quad c^{-1} + c'^{-1} = 1, \ c/c' = c - 1 > 0)$
mit $c = 8^{k-2}$ führt zu

$$
\Big| \sum_{0<|b|\le A} S(b,\alpha) \Big|^{8^{k-2}} \le (2A)^{8^{k-2}-1} \sum_{0<|b|\le A} |S(b,\alpha)|^{8^{k-2}},
$$

also mit (2.1.6) zu

$$
(2.2.1) \qquad \Big| \sum_{x \in I} e(f(x)\alpha) \Big|^{2 \cdot 8^{k-2}} = \mathrm{O}\Big(\max\Big(A^{8^{k-2}}, \ A^{8^{k-2}-1} \sum_{0<|b|\le A} |S(b,\alpha)|^{8^{k-2}} \Big) \Big).
$$

2.3 Für $0 < |b| \le A$ sei

$$
\begin{aligned}
|S(b,\alpha)|^{8^{k-2}} &= \Big| \sum_{x \in I(b)} e(bg(x)\alpha) \Big|^{8^{k-2}} \\
(2.3.1) \qquad &= \sum_y T(y,b)\ e(yb\alpha),
\end{aligned}
$$

wobei $T(y,b) \neq 0$ nach (2.1.4) nur für

$$|y| \leq 8^{k-2} \max_{x \in I(b)} |g(x,b)| = \mathrm{O}(A^{k-1}). \tag{2.3.2}$$

Mit den Orthogonalitätsrelationen, (2.3.1) und (2.1.5) folgt

$$\begin{aligned}
|T(y,b)| &= \Big| \int_0^1 \Big(\sum_{y'} T(y',b)\ e(y'b\alpha) \Big)\ e(-yb\alpha) d\alpha \Big| \\
&= \Big| \int_0^1 \Big| \sum_{x \in I(b)} e(bg(x,b)\alpha) \Big|^{8^{k-2}} e(-yb\alpha) d\alpha \Big| \\
&= \Big| \frac{1}{b} \int_0^b \Big| \sum_{x \in I(b)} e(g(x,b)\beta) \Big|^{8^{k-2}} e(-y\beta) d\beta \Big| \\
&= \Big| \int_0^1 \Big| \sum_{x \in I(b)} e(g(x,b)\alpha) \Big|^{8^{k-2}} e(-y\alpha) d\alpha \Big| \\
&\leq \int_0^1 \Big| \sum_{x \in I(b)} e(g(x,b)\alpha) \Big|^{8^{k-2}} d\alpha.
\end{aligned}$$

Im vorletzten Schritt wurde die 1–Periodizität des Integranden benutzt. Nach 2.1. kann auf das letzte Integral die Induktionsvoraussetzung angewandt werden.

$$T(y,b) = \mathrm{O}(A^{8^{k-2}-(k-1)}) \tag{2.3.3}$$

für $0 < |b| \leq A$ und (y gemäß (2.3.2)).

2.4. Mit (2.2.1) und (2.3.1) ergibt sich

$$\begin{aligned}
J_k &= \mathrm{O}\Big(\int_0^1 \Big(A^{4 \cdot 8^{k-2}} + A^{4 \cdot 8^{k-2} - 4} \Big(\sum_{0 < |b| \leq A} \Big| S(b,\alpha) \Big|^{8^{k-2}} \Big)^4 \Big) d\alpha \Big) \\
&= \mathrm{O}\Big(A^{4 \cdot 8^{k-2}} \Big) + \mathrm{O}\Big(A^{4 \cdot 8^{k-2} - 4} \cdot \int_0^1 \Big(\sum_{0 < |b| \leq A} \sum_{y} T(y,b)\ e(yb\alpha) \Big)^4 d\alpha \Big).
\end{aligned} \tag{2.4.1}$$

Das letzte Integral läßt sich nach (2.3.2) ausdrücken durch

$$\sum_{\substack{0 < |b_j| \leq A \\ y_1 b_1 + \ldots + y_4 b_4 = 0}} \ \sum_{|y_j| \leq C_3 A^{k-1}} T(y_1,b_1) \ldots T(y_4,b_4). \tag{2.4.2}$$

Benennt man y_3, y_4 um in $-z_3, -z_4$, und benutzt (2.3.3), so wird dieser Ausdruck zu

$$\begin{aligned}
\mathrm{O}\Big(A^{4 \cdot 8^{k-2} - 4(k-1)} \#\big\{ &(b_1, \ldots, b_4, y_1, y_2, z_1, z_2),\ \ 0 < |b_j| \leq A, \\
&|y_j|, |z_j| \leq C_3 A^{k-1}, b_1 y_1 + b_2 y_2 = b_3 z_3 + b_4 z_4 \big\} \Big).
\end{aligned} \tag{2.4.3}$$

Wie im ersten Induktionsschritt läßt sich die Anzahl der 8–Tupel in (2.4.3) abschätzen durch

$$\begin{aligned}
&\leq \sum_{|a|\leq 2C_3A^k} Q^2(a, A, C_3\ A^{k-1}) \\
&= \mathrm{O}\Big(A^3\ A^{3(k-1)} + \sum_{0<|a|\leq 2C_3A^k} A^2\ A^{2(k-1)}\ \Big(\sum_{d|a}\frac{1}{d}\Big)^2\Big) \\
&= \mathrm{O}(A^{3k}).
\end{aligned}$$

Zusammenfassung mit (2.4.1), ..., (2.4.3) ergibt schließlich

$$\begin{aligned}
J_k &= \mathrm{O}(A^{4\cdot 8^{k-2}}) + \mathrm{O}(A^{4\cdot 8^{k-2}-4+4\cdot 8^{k-2}-4k+4+3k}) \\
&= \mathrm{O}(A^{4\cdot 8^{k-2}}) + \mathrm{O}(A^{8^{k-1}-k}) = \mathrm{O}(A^{8^{k-1}-k}),
\end{aligned}$$

wie behauptet. □

Aus dem Bisherigen kann nun relativ rasch das Hauptergebnis gefolgert werden.

1.8. Satz von Waring–Hilbert.
Zu jedem $k \geq 2$ existiert ein $g(k)$, so daß jedes $n \in \mathbb{N}$ in der Form

$$n = x_1^k + \ldots + x_g^k \quad (x_j \in \mathbb{N}_0)$$

darstellbar ist.

Beweis.
1. Sei

$$L = \frac{1}{2}\ 8^{k-1}, \tag{1.1}$$

$$R(n) = \#\big\{(x_1, \ldots, x_L)\ \in \mathbb{N}_0^L,\ \ x_1^k + \ldots + x_L^k = n\big\}. \tag{1.2}$$

Alle folgenden $C_j(>0)$ können von k abhängen und sind im Prinzip explizit angebbar. Es gilt für $N \in \mathbb{N}$

$$\sum_{n\leq N} R(n) \geq C_4\ N^{L/k}. \tag{1.3}$$

Denn für $N \geq 2L$ ist

$$\begin{aligned}
\sum_{n\leq N} R(n) &= \sum_{0\leq a\leq N} \#\big\{(x_1, \ldots, x_L) \in \mathbb{N}_0^L,\ x_1^k + \ldots + x_L^k = a\big\} \quad - 1 \\
&\geq \Big(\#\big\{0 \leq x \leq \big(\frac{N}{L}\big)^{1/k}\big\}\Big)^L - 1 \\
&\geq \big(\frac{N}{L}\big)^{L/k} - 1 \geq C_5\ N^{L/k}.
\end{aligned}$$

Wegen $R(1) \geq 1$ gilt (1.3) für alle $N \geq 1$ mit einem $C_4 \in (0, C_5]$. Denn für $N \in [1, 2L]$ ist $\sum\limits_{n \leq N} R(n) \geq 1 \geq N^{4k}(2L)^{-L/k}$, also $C_4 = \min\big(C_5, (2L)^{-L/k}\big)$.

2. Für alle $N \geq 1$ besteht die Ungleichung

$$\sum_{n \leq N} R^2(n) \leq C_6 \; N^{2L/k-1}. \tag{2.1}$$

Denn sei

$$A = [N^{1/k}]. \tag{2.2}$$

Für $N \geq C_7$ ist nach (1.1)

$$M \underset{\text{Df}}{=} LA^k \geq N. \tag{2.3}$$

Wie schon mehrfach sieht man mit den Orthogonalitätsrelationen

$$\begin{aligned}
\sum_{n \leq N} R^2(n) &\leq \sum_{0 \leq a \leq M} \Big(\#\big\{(x_1, \ldots, x_L),\; 0 \leq x_j \leq A,\; x_1^k + \ldots + x_L^k = a\big\}\Big)^2 \\
&= \int_0^1 \Big| \sum_{0 \leq a \leq M} e(a\alpha) \#\big\{(x_1 \ldots, x_L),\; 0 \leq x_j \leq A,\; x_1^k + \ldots + x_L^k = a\big\}\Big|^2 d\alpha \\
&= \int_0^1 \Big| \sum_{0 \leq x_1, \ldots, x_L \leq A} e\big(\alpha(x_1^k + \ldots + x_L^k)\big)\Big|^2 d\alpha \\
&= \int_0^1 \Big| \sum_{0 \leq x \leq A} e(\alpha x^k)\Big|^{2L} d\alpha.
\end{aligned}$$

Das letzte Integral läßt sich nach Hilfssatz 1.7. durch

$$\mathrm{O}\Big(A^{8^{k-1}-k}\Big) = \mathrm{O}\Big(N^{2L/k-1}\Big)$$

abschätzen. Dies ist richtig für $N \geq C_7$, also mit eventuell vergrößerter O–Konstante für alle $N \geq 1$.

3. Der folgende Trick, bei dem 1. und 2. verwandt werden, ist im Zusammenhang mit dem Schnirelmanschen Satz oft anzutreffen. Die Cauchy–Schwarz–Ungleichung ergibt

$$\Big(\sum_{n \leq N} R(n)\Big)^2 \leq \Big(\sum_{n \leq N, R(n) > 0} 1\Big) \Big(\sum_{n \leq N} R^2(n)\Big),$$

also mit (1.3) und (2.1)

$$\sum_{n \leq N, R(n) > 0} 1 \geq C_8 \; N^{2Lk^{-1} - 2Lk^{-1} + 1} = C_8 \; N.$$

Die Menge

$$\{n, n \quad \text{ist die Summe von } \; L \; k\text{-ten Potenzen}\} = L\, \mathbb{P}_k$$

hat somit positive Dichte. Mit dem Satz von Schnirelman ergibt dies die Behauptung des Satzes. □

Selbstverständlich kann durch Verfolgen der Konstanten im vorangehenden Beweis für $g(k)$ eine explizite obere Schranke angegeben werden. Da sich astronomisch große Werte ergeben, ist der Aufwand nicht lohnend. Wesentlich besseres liefert die Hardy–Littlewoodsche Methode, zum Beispiel für

$$G(k) \underset{\text{Df}}{=} \min_{\ell} \left\{ \exists\, N_0\ \forall\, n \geq N_0\ \exists\, x_1, \ldots, x_\ell \in \mathbb{N}_0 :\ n = x_1^k + \ldots + x_\ell^k \right\}$$

die obere Schranke

$$G(k) \leq \ln k \cdot (3 + \mathrm{o}(1)) \quad (k \to \infty).$$

2. Kapitel. Analytischer Beweis des Primzahlsatzes

Vorbemerkung. Für diesen Abschnitt sind Grundkenntnisse in Funktionentheorie (insbesondere Holomorphie, Cauchyscher Satz) erforderlich.

Literatur: J. Brüdern, Einführung in die analytische Zahlentheorie, Springer 1991.

Am Beispiel des Primzahlsatzes

$$\pi(x) = \#\{p \leq x\} = \frac{x}{\ln x}\ (1 + \mathrm{o}(1)), \quad \text{bzw.}$$
$$\psi(x) = \sum_{n \leq x} \Lambda(n) = \sum_{p^k \leq x} \ln p = x(1 + \mathrm{o}(1))$$

soll das Grundprinzip der analytischen Zahlentheorie

a) elementar–zahlentheoretisches Problem (hier: $\psi(x) = ?$),

b) Studium einer erzeugenden Funktion, hier der Dirichlet–Reihe $\displaystyle\sum_{n=1}^{\infty} \Lambda(n)\, n^{-s}$ $(s = \sigma + it \in \mathbb{C};\ \ \sigma, t \in \mathbb{R},\ \sigma > 1)$,

c) Rückschluß von analytischen Eigenschaften der erzeugenden Funktion auf $\psi(x)$

demonstriert werden. Der Schritt c) wird hier mit einem erst jüngst gefundenen, besonders elegantem Hilfsmittel, dem Newmanschen Tauber–Satz vollzogen.

Eine Reihe der Gestalt $\sum_{n\in\mathbb{N}} a_n\ n^{-s}$ $(a_n \in \mathbb{C}, s$ komplexe Variable) wird als **Dirichlet–Reihe** bezeichnet. Die wichtigste von allen, auf die sich viele andere zurückführen lassen, ist die **Riemannsche Zeta–Funktion** (für reelle s schon von Euler benutzt, für komplexe s 1859 durch Riemann eingeführt).

2.1. Def. Die Reihe $\sum_{n=1}^{\infty} n^{-s}$ stellt eine für $\sigma = \mathrm{Re}\ s > 1$ holomorphe Funktion dar, die **Riemannsche Zeta–Funktion** $\zeta(s)$.

Beweis der Holomorphie. In jeder Halbebene $\sigma \geq 1+\varepsilon$ $(\varepsilon > 0)$ ist die Reihe wegen $|\sum_n n^{-s}| \leq \sum_n n^{-1-\varepsilon}$ gleichmäßig konvergent. Nach dem Konvergenzsatz von Weierstraß stellt sie eine in $\{s, \sigma > 1\}$ holomorphe Funktion dar. □

2.2. Satz. Die Funktion $\zeta(s) - \frac{1}{s-1}$ läßt sich in die Halbebene $\{s, \sigma > 0\}$ holomorph fortsetzen. Oder: $\zeta(s)$ ist – bis auf einen Pol erster Ordnung mit Residuum 1 – in $\{s, \sigma > 0\}$ holomorph fortsetzbar.

Beweis. Für $N \in \mathbb{N},\quad N > 1,\quad \sigma = \mathrm{Re}\ s > 1$ sieht man mit partieller Summation

$$\begin{aligned}\sum_{n\leq N} n^{-s} &= N \cdot N^{-s} - \int_1^N [t]\ \frac{d}{dt}(t^{-s})\ dt \\ &= N^{1-s} + s\int_1^N t^{-s}dt - s\int_1^N \{t\}\ t^{-s-1}\ dt \\ &= \frac{1}{1-s}N^{1-s} + 1 + \frac{1}{s-1} - s\int_1^N \{t\}\ t^{-s-1}\ dt.\end{aligned}$$

Für $N \to \infty$ fällt der erste Summand rechts fort, das letzte Integral konvergiert für $\sigma > 0$ kompakt gleichmäßig gegen eine holomorphe Funktion $I(s)$ also

$$\zeta(s) = \frac{1}{s-1} + 1 - s\ I(s).$$

$1 - s\ I(s)$ stellt somit die holomorphe Fortsetzung von $\zeta(s) - \dfrac{1}{s-1}$ in die Halbebene $\{s, \sigma > 0\}$ dar. □

2.3. Produktsatz für Dirichlet–Reihen.
Seien $f, g : \mathbb{N} \to \mathbb{C}$ zahlentheoretische Funktionen und $h = f * g$ (Faltprodukt). Die

Reihen $F(s) = \sum_n f(n)n^{-s}$ und $G(s) = \sum_n g(n)n^{-s}$ seien für $s \in D \subset \mathbb{C}$ absolut konvergent. Dann ist dort auch $H(s) = \sum_n h(n)n^{-s}$ absolut konvergent und es gilt

$$H(s) = F(s) \cdot G(s).$$

Beweis. Für jedes $s \in D$ kann nach dem Produktsatz für unendliche Reihen wegen der absoluten Konvergenz wie folgt umgeformt werden:

$$\begin{aligned} F(s) \cdot G(s) &= \sum_{n,m\in\mathbb{N}} f(n)\ g(m)\ (nm)^{-s} \\ &= \sum_{k\in\mathbb{N}} k^{-s} \sum_{n,m,n\cdot m=k} f(n)\ g(m) \\ &= \sum_{k\in\mathbb{N}} h(k)\ k^{-s} = H(s). \end{aligned}$$

□

2.4. Beispiele. Für $\sigma > 1$ gilt

1) $$\sum_{n=1}^{\infty} \mu(n)\ n^{-s} = 1/\zeta(s),$$

insbesondere hat $\zeta(s)$ in $\{s, \sigma > 1\}$ keine Nullstelle.

2) $$\sum_{n\in\mathbb{N}} \Lambda(n)\ n^{-s} = -\zeta'(s)/\zeta(s).$$

Beide Reihen stellen in $\{s, \sigma > 1\}$ holomorphe Funktionen dar.

Beweis.
1) Wegen $|\mu(n)| \leq 1$ liefert $\sum \mu(n)\ n^{-s}$ eine in $D = \{s, \sigma > 1\}$ absolut konvergente Dirichlet–Reihe und holomorphe Funktion. Mit 2.3 erhält man

$$\zeta(s) \cdot \sum_n \mu(n)\ n^{-s} = \sum_k (1 * \mu)(k)\ k^{-s} = \sum_k \varepsilon(k)\ k^{-s} = 1.$$

Hätte ζ in D eine Nullstelle, dann könnte die Identität nur gelten, wenn $\sum \mu(n)\ n^{-s}$ dort einen Pol hätte, was aber wegen der Holomorphie ausgeschlossen ist. □

2) In G kann $\zeta(s)$ gliedweise differenziert werden.
Wegen $\frac{d}{ds} n^{-s} = \frac{d}{ds} \exp(-s \ln n) = -\ln n \cdot n^{-s}$ ist

$$\zeta'(s) = -\sum_n \ln n \cdot n^{-s}.$$

Mit 2.3., $\Lambda = \mu * \ln$ und 1) erhält man in G

$$\frac{1}{\zeta(s)} \cdot \big(-\zeta'(s)\big) = \sum_n \mu(n)\ n^{-s} \cdot \sum_m \ln m \cdot m^{-s} = \sum_k \Lambda(k)\ k^{-s}.$$

□

Die Bedeutung der Zeta–Funktion für die Verteilung der Primzahlen wird auch deutlich durch das sogenannte **Euler–Produkt**

$$\zeta(s) = \prod_p (1 - p^{-s})^{-1} \qquad (\text{Re } s > 1).$$

Die Gestalt der Reihe $\sum_n \Lambda(n)\, n^{-s}$ zeigt, daß für das analytische Verhalten, insbesondere die analytische Fortsetzbarkeit nach links, das Nicht–Verschwinden der ζ–Funktion von entscheidender Bedeutung ist. Schon die Aussage $\zeta(1+it) \neq 0 \quad (t \neq 0)$ erfordert einiges an neuen Ideen. Bis heute ist kein einfacher Beweis hierfür bekannt. Die folgende Methode geht auf de la Vallée–Poussin zurück.

2.5. Satz (Hadamard, de la Vallée–Poussin, (1896)).

$$\zeta(1+it) \neq 0 \quad \text{für alle} \quad t \neq 0.$$

Beweis.
1. Für $\varphi \in \mathbb{R}$ gilt

$$3 + 4\cos\varphi + \cos(2\varphi) = 2(1+\cos\varphi)^2 \geq 0.$$

2. Für $\sigma > 1,\ t \neq 0$ sieht man mit 2.4.2)

$$\begin{aligned} &\text{Re}\Big(3\frac{\zeta'}{\zeta}(\sigma) + 4\ \frac{\zeta'}{\zeta}(\sigma+it) + \frac{\zeta'}{\zeta}(\sigma+2it)\Big) \\ &= -\text{Re}\ \sum_n \frac{\Lambda(n)}{n^\sigma}\ \big(3 + 4\ n^{-it} + n^{-2it}\big) \\ &= -\sum_n \frac{\Lambda(n)}{n^\sigma}\big(3 + 4\cos(-t\ln n) + \cos(-2t\ln n)\big) \quad \leq 0. \end{aligned}$$

3. Angenommen, ζ verschwinde bei $1+it$ von m–ter Ordnung,

$$\zeta(\sigma+it) = (\sigma-1)^m\ \tilde{h}_1\ (\sigma-1) \qquad (\sigma > 1)$$

mit in einer Umgebung der Null differenzierbarem $\tilde{h}_1$ und $\tilde{h}_1(0) \neq 0$. Dann folgt

$$\frac{\zeta'}{\zeta}(\sigma+it) = \frac{m}{\sigma-1} + h_1(\sigma-1) \tag{3.1}$$

mit auf [1,2] beschränktem h_1. Analog sieht man, wenn ζ bei $1+2it$ von μ–ter Ordnung $(\mu \geq 0)$ verschwindet,

$$\frac{\zeta'}{\zeta}(\sigma + 2it) = \frac{\mu}{\sigma - 1} + h_2(\sigma - 1). \tag{3.2}$$

Wegen des Pols bei 1 ist

$$\frac{\zeta'}{\zeta}(\sigma) = \frac{-1}{\sigma - 1} + h_0(\sigma - 1) \tag{3.3}$$

mit beschränktem $h_0 \quad (1 \leq \sigma \leq 2)$.

4. 2. und 3. zusammen ergeben

$$\begin{aligned} 0 &\geq \text{Re}\left(\frac{-3 + 4m + \mu}{\sigma - 1} + \text{ Beschränktes}\right) \\ &= \frac{-3 + 4m + \mu}{\sigma - 1} + \text{ Beschränktes.} \end{aligned}$$

Für $\sigma \to 1^+$ wird die rechte Seite wegen $m \geq 1$ beliebig groß, insbesondere positiv, was einen Widerspruch bedeutet. □

2.6. Folgerung. Die Funktion $-\frac{\zeta'}{\zeta}(s) - \frac{1}{s-1}$ ist holomorph fortsetzbar in ein Gebiet, das die abgeschlossene Halbebene $\{s, \sigma \geq 1\}$ umfaßt.

Beweis. Der Pol von ζ bei $s = 1$ bewirkt einen Pol erster Ordnung mit Residuum -1 zu ζ'/ζ. Also ist $-\frac{\zeta'}{\zeta}(s) - \frac{1}{s-1}$ holomorph in eine Umgebung von $s = 1$ fortsetzbar. Die Holomorphie in allen übrigen Punkten der 1–Geraden folgt aus dem vorigen Satz. □

Die Aussage von 2.6. wird sich als ausreichend für die Anwendung des Newmanschen Tauber–Satzes herausstellen.

Es ist oft einfacher, von der Koeffizientenfolge einer Potenz– oder Dirichlet–Reihe auf die Eigenschaften der Reihe zu schließen, als umgekehrt. Als Beispiel der **Satz von Abel.** Sei $(a_n)_{n\in\mathbb{N}}$ eine komplexe Zahlenfolge, für die $\sum\limits_n a_n$ gegen $a \neq 0$ konvergiert. Die Potenzreihe $A(z) = \sum\limits_n a_n \, z^n$ habe den Konvergenzradius 1. Dann ist die Funktion $A(t) \quad (-1 < t < 1)$ stetig in den Punkt $t = 1$ fortsetzbar und hat dort den Wert a.

Die Umkehrung (aus der Stetigkeit auf die Konvergenz von $\sum a_n$ schließen) ist nur unter Zusatzbedingungen möglich. Sätze, in denen aus dem Stetigkeits– oder Holomorphieverhalten, insbesondere am Rand des Konvergenzbereichs, auf das Grenzwertverhalten der Koeffizienten geschlossen wird, heißen **Tauber–Sätze** (benannt nach Alfred Tauber, 1866–1942, umgekommen im KZ Theresienstadt).

Der 1980 von Donald J. Newman gefundene Tauber–Satz kommt mit wenig einschneidenden Bedingungen aus und ist für Laplace–Transformierte formuliert.

2.7. Newmanscher Tauber–Satz (1980).
Sei $f : [0, \infty) \to \mathbb{C}$, beschränkt und auf jedem Intervall $[0, a]$ Riemann–integrierbar. Dann stellt

$$F(z) = \int_0^\infty f(t)\, e^{-zt}\, dt \qquad \text{(Laplace–Transformierte von } f\text{)}$$

eine für Re $z > 0$ holomorphe Funktion dar.

Es sei F analytisch fortsetzbar in ein Gebiet, das die imaginäre Achse umfaßt. Dann gilt:

$$\int_0^\infty f(t)\, dt \quad \text{existiert (und hat den Wert } F(0)\text{).}$$

Beweis.
1. Für $0 < \lambda < \infty$ sei

$$F_\lambda(z) = \int_0^\lambda f(t)\, e^{-zt}\, dt$$

F_λ ist offenbar eine auf ganz $\mathbb{C}$ holomorphe Funktion. Es reicht zu zeigen, daß

$$F_\lambda(0) = \int_0^\lambda f(t)\, dt \to F(0) \quad \text{für} \quad \lambda \to \infty.$$

Oder, wenn $\varepsilon > 0$ vorgegeben ist,

$$|F_\lambda(0) - F(0)| < \varepsilon \quad \text{für} \quad \lambda \geq \lambda_0(\varepsilon). \tag{1}$$

2. Es werde $R > 0$ vorläufig beliebig gewählt, später in Abhängigkeit von ε genügend groß. Nach Voraussetzung gibt es ein $\delta = \delta(R) > 0$, so daß F holomorph ist für

$$\text{Re } z \geq -\delta, \quad |\text{Im } z| \leq R.$$

Sei $W = W(R)$ folgender geschlossener Weg, positiv umlaufen.

a) Der Halbkreis vom Radius R um $z_0 = 0$ in der rechten Halbebene (W^+).

b) Der Rechteckweg von iR nach $iR - \delta$, von $iR - \delta$ nach $-iR - \delta$ und von $-iR - \delta$ nach $-iR$ (W^-).

Dann bewirkt die Cauchysche Integralformel

$$F(0) - F_\lambda(0) = \frac{1}{2\pi i} \int\limits_W (F(z) - F_\lambda(z)) \cdot e^{\lambda z} \Big(\frac{1}{z} + \frac{z}{R^2} \Big) dz. \tag{2}$$

Die Verwendung dieses Integranden ist als der eigentliche Beweistrick anzusehen. Er erlaubt es, das Integral auf W gut abzuschätzen. Die Standard–Anwendung der Cauchy'schen Formel mit dem Integranden $(F(z) - F_\lambda(z))\frac{1}{z}$ würde zu Schwierigkeiten führen.

3. Nach Voraussetzung kann

$$|f(t)| \le A \qquad \forall\, t \ge 0$$

benutzt werden. Für $x = \mathrm{Re}\ z > 0$ und $|z| = R$ ist

$$\frac{1}{z} + \frac{z}{R^2} = \frac{x - iy}{x^2 + y^2} + \frac{x + iy}{R^2} = \frac{2x}{R^2},$$

$$|F(z) - F_\lambda(z)| = \Big| \int\limits_\lambda^\infty f(t)\ e^{-zt}\ dt \Big| \le A \int\limits_\lambda^\infty e^{-xt}\ dt = \frac{A}{x}\ e^{-\lambda x}.$$

Damit läßt sich der Integrand in (2) für $\mathrm{Re}\ z > 0$ im Betrag abschätzen durch

$$\frac{A}{x}\ e^{-\lambda x}\ e^{\lambda x}\ \frac{2x}{R^2} = \frac{2A}{R^2}.$$

Dies ergibt

$$\Big| \frac{1}{2\pi i} \int\limits_{W^+} \dots \Big| \le \frac{A}{R}. \tag{3}$$

4. Bei $-F_\lambda$ wird W^- deformiert zu dem Halbkreis vom Radius R in der linken Halbebene. Wie in 3. erhält man dort

$$|F_\lambda(z)| \le A \int\limits_0^\lambda e^{-xt}\ dt\ < \frac{Ae^{-\lambda x}}{|x|}$$

und

$$\Big| \frac{1}{2\pi i} \int\limits_{W^-} (-F_\lambda(z))\ e^{\lambda z} \Big(\frac{1}{z} + \frac{z}{R^2} \Big) dz \Big| < \frac{A}{R}. \tag{4}$$

5. Es bleibt der Beitrag von $F(z)$ über W^- .
Die Funktion $F(z)\big(\frac{1}{z} + \frac{z}{R^2}\big)$ ist auf dem Kompaktum $Sp(W^-)$ holomorph und somit

durch $B = B(R)$ beschränkt.
Das F–Integral über die Vertikale von W^- ist daher

$$(5.1) \qquad |\quad| \le \frac{1}{\pi}\, BR\, e^{-\delta\lambda}.$$

Die Integrale über die Horizontalen sind

$$(5.2) \qquad |\quad| \le \frac{B}{\pi} \int_{-\delta}^{0} e^{x\lambda}\, dx < \frac{B}{\pi\lambda}.$$

6. Zusammenfassung liefert für beliebiges R und $\lambda > 0$

$$(6) \qquad |F(0) - F_\lambda(0)| < \frac{2A}{R} + B(R)\, \Big(R\frac{1}{\pi}\, e^{-\delta\lambda} + \frac{1}{\pi\lambda}\Big).$$

Es werde als erstes R so groß gewählt, daß $\frac{2A}{R} < \frac{\varepsilon}{2}$. Für jetzt festgehaltenes R (und damit fixe $B(R)$ und δ) gilt $\lim\limits_{\lambda\to\infty} \big(\frac{R}{\pi}\, e^{-\delta\lambda} + \frac{1}{\pi\lambda}\big) = 0$, für $\lambda \ge \lambda_0(\varepsilon)$ ist daher der zweite Teil rechts in (6) $< \frac{\varepsilon}{2}$. Damit ist nach (1) der Beweis geführt. □

Es ist nun nicht mehr weit bis zum Ziel des Abschnittes

2.8. Primzahlsatz. Es gilt $\lim\limits_{x\to\infty} \dfrac{\psi(x)}{x} = 1$ bzw. $\lim\limits_{x\to\infty} \dfrac{\pi(x)}{x/\ln x} = 1.$

Es wird die ψ–Aussage bewiesen und zum Abschluß die π–Aussage gefolgert.

1. Für $\sigma = \operatorname{Re} s > 1$ und $N \in \mathbb{N}$ folgt mit partieller Summation

$$\sum_{n\le N} \Lambda(n)\, n^{-s} = \psi(N)\, N^{-s} + s \int_1^N \psi(u)\, u^{-s-1}\, du.$$

Die Substitution $t = \ln u$ macht das Integral zu

$$\int_0^{\ln N} \psi(e^t)\, e^{-t}\, e^{-t(s-1)}\, dt.$$

Für $N \to \infty$ geht wegen $\psi(N) = \mathrm{O}(N)$ der Term $\psi(N)\, N^{-s}$ gegen Null, $\sum\limits_{n\le N} \Lambda(n)\, n^{-s}$ wird nach 2.4.(2) zu $-\zeta'(s)/\zeta(s)$, das Integral konvergiert, also

$$-\frac{\zeta'}{\zeta}(s) \cdot \frac{1}{s} = \int_0^\infty \frac{\psi(e^t)}{e^t}\, e^{-t(s-1)}\, dt \qquad (\sigma > 1).$$

Setzt man $z = s - 1$, dann folgt hieraus

$$(1) \qquad -\frac{1}{z+1}\,\frac{\zeta'}{\zeta}(z+1) = \int\limits_0^\infty \frac{\psi(e^t)}{e^t}\, e^{-tz}\, dt \qquad (\mathrm{Re}\ z > 0).$$

2. In ähnlicher Weise sieht man

$$\frac{1}{z+1}\,\zeta(z+1) = \int\limits_0^\infty \frac{[e^t]}{e^t}\, e^{-tz}\, dt \qquad (\mathrm{Re}\ z > 0).$$

3. Nach 2.2. und 2.6. ist

$$-\frac{\zeta'}{\zeta}(z+1) - \zeta(z+1) \quad \text{holomorph für} \quad \mathrm{Re}\ z \geq 0.$$

Es kann somit im Hinblick auf den Tauber–Satz

$$F(z) = \frac{1}{z+1}\Big(-\frac{\zeta'}{\zeta}(z+1) - \zeta(z+1)\Big) = \int\limits_0^\infty \Big(\frac{\psi(e^t)}{e^t} - \frac{[e^t]}{e^t}\Big)\, e^{-tz}\, dt$$

geschrieben werden. Wegen $\psi(e^t) = O(e^t)$ ist $f(t) = e^{-t}(\psi(e^t) - [e^t])$ beschränkt (und offenbar auf jedem Intervall integrierbar). Es kann der Tauber–Satz angewandt werden:

$$\int\limits_0^\infty e^{-t}(\psi(e^t) - [e^t])\, dt \quad \text{konvergiert.}$$

Ersetzt man $[e^t]$ durch $e^t - \{e^t\}$ und berücksichtigt die Konvergenz von $\displaystyle\int\limits_0^\infty e^{-t}\,\{e^t\}\, dt$, dann hat man

$$(3) \qquad \int\limits_0^\infty \big(\psi(e^t)\, e^{-t} - 1\big)\, dt \quad \text{konvergiert.}$$

4. Aus (3) folgt $\psi(e^t)\, e^{-t} \to 1$. Es werde z.B. angenommen, daß

$$\overline{\lim_{t\to\infty}}\ \psi(e^t)\, e^{-t} > 1$$

ist. Dies bedeutet, daß es eine gegen ∞ divergierende Folge (t_ν) und ein $\delta > 0$ gibt, so daß

$$\forall\ \nu : \psi(e^{t_\nu}) \geq e^{t_\nu}\ (1+\delta).$$

Mit einem (kleinen) $c > 0$ folgt daraus für jedes ν

$$\int_{t_\nu}^{t_\nu+c} \big(\psi(e^t)/e^t - 1\big)dt \geq \int_{t_\nu}^{t_\nu+c} \big(e^{t_\nu}(1+\delta)/e^{t_\nu+c}\big)\, dt - c = c\big((1+\delta)\, e^{-c} - 1\big).$$

Dies ist $\geq \frac{1}{2}\, c\delta$, wenn $c = c(\delta)$ genügend klein gewählt wird. Wegen der Konvergenz des Integrals müßte $\int_{t_\nu}^{t_\nu+c} \ldots$ gegen Null konvergieren.

Ähnlich argumentiert man bei der Annahme $\underline{\lim}\, \psi(e^t)\, e^{-t} < 1$.

Damit ist der Primzahlsatz in der ψ–Version gezeigt.

5. Wegen

$$\begin{aligned} 0 \leq \sum_{p^k \leq x, k \geq 2} \ln p &= \sum_{p \leq x^{1/2}} \ln p \sum_{k \geq 2, p^k \leq x} 1 \\ &\leq \sum_{p \leq x^{1/2}} \ln p \cdot \frac{\ln x}{\ln p} \leq x^{1/2} \ln x = \mathrm{o}(x) \end{aligned}$$

gilt.

$$\vartheta(x) \underset{\mathrm{Df}}{=} \sum_{p \leq x} \ln p = \psi(x) - \sum_{p^k \leq x, k \geq 2} \ln p = x + \mathrm{o}(x)$$

nach dem oben Bewiesenen. Oder

$$\vartheta(x) = x + \varepsilon(x) \cdot x \quad \text{mit} \quad \varepsilon(x) \to 0 \quad \text{für} \quad x \to \infty. \tag{5.1}$$

$\pi(x) = \sum_{p \leq x} \ln p \cdot \frac{1}{\ln p}$ kann daraus durch partielle Summation bestimmt werden. Sei

$$f(n) = \begin{cases} \ln p, & \text{falls} \quad n = p \\ 0 & \text{sonst} \end{cases}$$

$$F(t) = \sum_{n \leq t} f(n) = \vartheta(t) = \begin{cases} 0 & \text{für} \quad 1 \leq t < 2, \\ t + t\varepsilon(t) & \text{für} \quad t \geq 2. \end{cases}$$

$$g(t) = \begin{cases} (\ln t)^{-1} & \text{für} \quad t \geq 2 \\ \text{irgendwie stetig differenzierbar bis} & t = 1 \quad \text{fortgesetzt.} \end{cases}$$

Dann erhält man

$$\pi(x) = \frac{\vartheta(x)}{\ln x} + \int_2^x \vartheta(t)\, \frac{1}{t \ln^2 t} dt \tag{5.2}$$

Im Integral kann grob durch $\big|\vartheta(t)\big| \le Ct$ mit einem $C > 0$ abgeschätzt werden. Man erhält für das Integral die Betragsschranke

$$C \int\limits_2^x \frac{dt}{\ln^2 t} \le C\Big(\int\limits_2^{x^{1/2}} \frac{dt}{\ln^2 t} + 4 \int\limits_{x^{1/2}}^x \frac{dt}{\ln^2 x} \Big) = \mathrm{O}\Big(\frac{x}{\ln^2 x}\Big).$$

Mit (5.1) und (5.2) ergibt das

$$\pi(x) = \frac{x}{\ln x} + \varepsilon(x)\ \frac{x}{\ln x} + \mathrm{O}\Big(\frac{x}{\ln^2 x}\Big) = \frac{x}{\ln x} + \mathrm{o}\Big(\frac{x}{\ln x}\Big),$$

wie behauptet.

3. Kapitel. Algebraische und transzendente Zahlen.

Literatur:
A. Baker, Transzendental Number Theory, Cambridge University Press, 1975.
P. Bundschuh, Einführung in die Zahlentheorie, Springer 1988.

Für einen kommutativen, Nullteiler–freien Ring R mit Eins bezeichne $R[x_1, \ldots, x_n]$ den Ring der Polynome über R in n Unbestimmten $x_1, \ldots, x_n$. Ein Polynom $f(x) = a_n\ x^n + \ldots + a_0 \in R[x]$ mit $a_n \neq 0$ heißt **normiert**, wenn der Leitkoeffizient $a_n = 1$ ist. Ist R ein Körper, dann kann $f(x)$ mit $a_n \neq 0$ durch Division durch a_n normiert werden.

3.1. Def. und Folgerungen.

(1) Def. $\alpha \in \mathbb{C}$ heißt **algebraisch** (algebraische Zahl), wenn es ein Polynom

$$f(x) = x^n + a_{n-1}\ x^{n-1} + \ldots + a_0 \in \mathbb{Q}[x]$$

$(n \in \mathbb{N})$ gibt mit $f(\alpha) = 0$.

(2) Folg. und Def. α algebraisch. Dann existiert ein eindeutig bestimmtes, über $\mathbb{Q}$ irreduzibles Polynom

$$p(x) = x^n + b_{n-1}\ x^{n-1} + \ldots + b_0 \in \mathbb{Q}[x]$$

mit $n \in \mathbb{N}$ und $p(\alpha) = 0$. p heißt das **Minimalpolynom** von α, α heißt **algebraisch vom Grad** n.
Hinweis. Es existiert ein $p(x) \in \mathbb{Q}[x]$, das normiert ist, α als Nullstelle hat, und über $\mathbb{Q}$ irreduzibel ist, z.B. eins mit minimalem Grad. Angenommen, es gibt ein zweites mit

diesen Eigenschaften, $q(x)$. Da $\mathbb{Q}$ Körper ist, kann in $\mathbb{Q}[x]$ Polynomdivision durchgeführt werden:

$$q(x) = a(x)\ p(x) + r(x), \quad \text{Grad}\ \ r < n.$$

Aus $p(\alpha) = q(\alpha) = 0$ folgt $r(\alpha) = 0$. Wäre r nicht das Nullpolynom, hätte man einen Widerspruch zur Minimalität des Grades von p. Bleibt $q = ap$. Wegen der Irreduzibilität und Normiertheit von q und p bleibt nur $p = q$.

(3) Def. Die algebraische Zahl α heißt **ganz–algebraisch**, wenn das Minimalpolynom in $\mathbb{Z}[x]$ liegt.

Bsp. Die $\alpha \in \mathbb{Z}$ sind genau die ganz–algebraischen Zahlen vom Grad 1, $\sqrt{2}$ ist ganz–algebraisch vom Grad 2.

(4) Folg. α algebraisch. Dann existiert ein $d \in \mathbb{N}$, so daß $d\alpha$ ganz–algebraisch ist.

Beweis. Sei

$$p(\alpha) = \alpha^n + a_{n-1}\ \alpha^{n-1} + \ldots + a_0 = 0 \qquad (a_j \in \mathbb{Q}).$$

Man wähle als d das kgV der Nenner der Zahlen $a_0, \ldots, a_{n-1}$. Dann ist

$$p_1(d\alpha) = (d\alpha)^n + da_{n-1}(d\alpha)^{n-1} + \ldots + d^{n-1}a_1(d\alpha) + d^n\ a_0 = 0.$$

Die Koeffizienten von p_1 liegen in $\mathbb{Z}$, mit p ist auch p_1 irreduzibel. Denn wegen $p_1(dx) = d^n\ p(x)$ ergäbe eine Zerlegung von p_1 eine von p. □

(5) Def. Das Minimalpolynom von α zerfalle über $\mathbb{C}$ wie folgt

$$p(x) = (x - \alpha^{(1)}) \cdot \ldots \cdot (x - \alpha^{(n)}), \quad \alpha = \alpha^{(1)}.$$

$\alpha^{(2)}, \ldots, \alpha^{(n)}$ heißen die **Konjugierten** von α.

(6) Folg. $\alpha, \alpha^{(2)}, \ldots, \alpha^{(n)}$ sind paarweise verschieden.

Beweis. Wie in $\mathbb{Z}$ kann in $\mathbb{Q}[x]$ ein ggT definiert und mit dem Euklidischen Algorithmus berechnet werden. Zu $f(x), g(x)$ gibt es ein $h(x)$ mit $h|f,\ h|g$ und für alle t mit $t|f,\ t|g$ gilt $t|h$. In normierter Form ist $h = \text{ggT}\ (f, g)$ eindeutig bestimmt.

Angenommen, α sei mehrfache Nullstelle von p. Dann ist α Nullstelle von $p'(x) \in \mathbb{Q}[x]$. Grad $p' = \text{Grad}\ p - 1$. Wie in $\mathbb{Z}$ sieht man, daß für den ggT h zweier Polynome f und g eine Darstellung

$$h = qf + rg \quad \big(q(x), r(x) \in \mathbb{Q}[x]\big)$$

existiert. Hieraus folgt, daß α Nullstelle des ggT h von p und p' ist. Da h ein Polynom ungleich dem Nullpolynom von kleinerem Grad als p ist, bedeutet dies einen Widerspruch.

□

(7) Folg. $\mathbb{A}$, die Menge aller algebraischen Zahlen, ist ein Körper, echter Oberkörper von $\mathbb{Q}$ und echter Teilkörper von $\mathbb{C}$.

Hinweis. Die Körpereigenschaft wird sich mit Hilfe des Satzes 3.8. über symmetrische Polynome ergeben, die zweite Aussage folgt unmittelbar aus Satz 3.3.

3.2. Def. $\alpha \in \mathbb{C}$ heißt **transzendent**, wenn es nicht algebraisch ist.

Die einfachste Methode, die Existenz transzendenter Zahlen zu zeigen, geht auf Georg Cantor (1845–1918) zurück. Sie liefert keine konkrete transzendente Zahl.

3.3. Satz von Cantor. Die Menge $\mathbb{A}$ der algebraischen Zahlen ist abzählbar. Es gibt transzendente Zahlen.

Beweis. Da jedes $\alpha \in \mathbb{A}$ Nullstelle eines $f(x) \in \mathbb{Z}[x]$ ist, reicht es, solche Polynome zu betrachten. Für $f(x) = a_n\, x^n + \ldots + a_0 \in \mathbb{Z}[x]$ sei

$$G(f) \underset{\text{Df}}{=} n + |a_n| + \ldots + |a_0| \in \mathbb{N}$$

(für $f \neq$ dem Nullpolynom). Zu jedem $N \in \mathbb{N}$ gibt es nur endlich viele f mit $G(f) = N$, also nur endlich viele α, für die $f(\alpha) = 0$ mit $f(x) \in \mathbb{Z}[x]$ und $G(f) = N$. Auf die Weise kann $\mathbb{A}$ abgezählt werden. Wegen der Überabzählbarkeit von $\mathbb{C}$ ist $\mathbb{C}\backslash\mathbb{A}$ nicht leer. □

Der chronologisch erste Beweis für die Existenz transzendenter Zahlen stammt von Liouville und beruht auf der Beobachtung, daß algebraische Zahlen sich nicht extrem gut durch rationale Zahlen approxomieren lassen.

3.4. Satz von Liouville (1844).
(1) Sei α algebraisch vom Grad $n > 1$. Dann existiert ein $C = C(\alpha) > 0$, so daß für alle $b/k \in \mathbb{Q}$ gilt

$$\left|\alpha - \frac{b}{k}\right| > C\; k^{-n}.$$

(2) Sei $\alpha \in \mathbb{C}\backslash\mathbb{Q}$. Existieren zu jedem $\varepsilon > 0$ und $n > 1$ $b \in \mathbb{Z}$ und $k \in \mathbb{N}$ mit

$$\left|\alpha - \frac{b}{k}\right| \leq \varepsilon\; k^{-n},$$

dann ist α transzendent.
Beweis zu (1). Es reicht, b/k mit $\left|\alpha - \frac{b}{k}\right| < 1$ zu betrachten. α ist Nullstelle des über $\mathbb{Q}$ irreduziblen Polynoms

$$f(x) = a_n\, x^n + \ldots + a_0 \in \mathbb{Z}[x], \quad n \geq 2.$$

Nach dem Mittelwertsatz der Differentialrechnung existiert ein ξ zwischen α und b/k mit

(a) $-f(b/k) = f(\alpha) - f(b/k) = (\alpha - b/k)\ f'(\xi)$.
Wegen $|\xi| \le 1 + |\alpha|$ ist

(b) $|f'(\xi)| \le C_1 = C_1(\alpha)$.

Da $n \ge 2$ und f irreduzibel, hat f nur irrationale Nullstellen. $f(b/k)k^n$ ist eine ganze Zahl $\neq 0$, also $|f(b/k)| \ge k^{-n}$. Mit (a) und (b) ergibt das

$$|\alpha - b/k| \ge C_1^{-1}\ k^{-n},$$

was der Behauptung entspricht. (2) folgt direkt aus (1). □

Bemerkungen.

1. Reelle α, die durch sehr rasch konvergente Reihen dargestellt werden, erweisen sich nach Liouville als transzendent, z.B.

$$\alpha = \sum_{\nu=1}^{\infty} 2^{-\nu!}.$$

Denn sei

$$\alpha_\ell = \sum_{\nu=1}^{\ell} 2^{-\nu!} = \frac{b_\ell}{k_\ell}, \qquad k_\ell = 2^{\ell!}.$$

Dann ist

$$|\alpha - \alpha_\ell| = \sum_{\nu=\ell+1}^{\infty} 2^{-\nu!} < 2^{-(\ell+1)!} \cdot 2 = 2\ k_\ell^{-(\ell+1)}.$$

Da $k_\ell \to \infty$ $(\ell \to \infty)$, ist die Bedingung in (2) erfüllt. □

2. Zahlen, die nach (2) transzendent sind, werden **Liouville–Zahlen** genannt. Man überlegt sich leicht, daß sie eine überabzählbare Teilmenge von $\mathbb{R}$ vom (Lebesgue–)Maß Null bilden. Nach dem Cantorschen Satz erfaßt man auf die Weise nur einen geringen Teil aller reellen, transzendenten Zahlen.

Da für e und π rasch konvergente Reihen bekannt sind und insbesondere für π immer noch neue gefunden werden, könnte man hoffen, daß die Transzendenz von e und π nach Liouville gezeigt werden kann. Dies ist nicht der Fall (für π: Kurt Mahler, 1952).

3. Der Approximationssatz von Liouville wurde mehrfach verschärft. Einen Schlußpunkt der Entwicklung bildete der

Satz von Roth (1955).
Sei α algebraisch vom Grad $n \geq 3$. Dann existieren zu jedem $\varepsilon > 0$ und jedem $C > 0$ nur endlich viele $b/k \in \mathbb{Q}$ mit

$$|\alpha - b/k| \leq C\ k^{-2-\varepsilon}.$$

Zu der Frage nach einer effektiven Abschätzung für die Anzahl der b/k und Größe der k gibt es bislang nur Teilergebnisse.

Einen der Höhepunkte der Zahlentheorie im 19. Jahrhundert stellt Hermite's Beweis der Transzendenz von e dar.

3.5. Satz von Hermite (1873, Charles H., 1822–1901).
Die Zahl $e = 2,71828\ldots$ ist transzendent.

Zuerst ein Hilfssatz, der auch bei π nützlich sein wird.

3.6. Hilfssatz. Sei

$$f(x) = \sum_{\nu=0}^{n} a_\nu\ x^\nu\ \in \mathbb{Z}[x],$$
$$F(x) = \sum_{\mu=0}^{n} f^{(\mu)}(x), \quad G(x) = F(0)\ e^x - F(x).$$

Dann gilt für $\alpha \in \mathbb{C}$

$$|G(\alpha)| \leq e^{|\alpha|} \sum_{\nu=0}^{n} |a_\nu|\ |\alpha|^\nu.$$

Beweis. Nach Definition ist

$$F(x) = \sum_{\mu=0}^{n} \sum_{\nu=\mu}^{n} a_\nu\ \frac{\nu!}{(\nu-\mu)!}\ x^{\nu-\mu}$$
$$= \sum_{\nu=0}^{n} a_\nu \sum_{\mu=0}^{\nu} \frac{\nu!}{(\nu-\mu)!} x^{\nu-\mu} = \sum_{\nu=0}^{n} a_\nu \sum_{\mu=0}^{\nu} \frac{\nu!}{\mu!}\ x^\mu,$$

also insbesondere

$$F(0) = \sum_{\nu=0}^{n} a_\nu\ \nu!.$$

Daraus ergibt sich

$$\begin{aligned}
|G(\alpha)| &= \Big| \sum_{\nu=0}^{n} a_\nu \sum_{\mu=0}^{\infty} \frac{\nu!}{\mu!}\, \alpha^\mu - \sum_{\nu=0}^{n} a_\nu \sum_{\mu=0}^{\nu} \frac{\nu!}{\mu!}\, \alpha^\mu \Big| \\
&= \Big| \sum_{\nu=0}^{n} a_\nu \sum_{\mu=\nu+1}^{\infty} \frac{\nu!}{\mu!}\, \alpha^\mu \Big| \\
&\le \sum_{\nu=0}^{n} |a_\nu| \sum_{\mu=\nu+1}^{\infty} \frac{|\alpha|^\mu}{(\mu-\nu)!} = \sum_{\nu=0}^{n} |a_\nu| \ |\alpha|^\nu \sum_{\kappa=1}^{\infty} \frac{|\alpha|^\kappa}{\kappa!} \\
&< e^{|\alpha|} \sum_{\nu=0}^{n} |a_\nu| \ |\alpha|^\nu .
\end{aligned}$$

□

Beweis zum Satz von Hermite. Die Grundidee des Beweises, und diese tritt in der Transzendenztheorie immer wieder auf, ist, unter Annahme der Algebraizität einen Ausdruck zu definieren, der analytisch nach oben und zahlentheoretisch nach unten abgeschätzt werden kann. Einen solchen Ausdruck zu finden, erfordert ein hohes Maß an Intuition.

1. Angenommen, e sei algebraisch und habe als Minimalpolynom

$$g(x) = b_0 + \ldots + b_m\, x^m \in \mathbb{Z}[x], \quad b_m \neq 0.$$

2. Für ein später hinreichend groß zu wählendes primes

$$p > \max(m, |b_0|) \tag{2.1}$$

setze man

$$\begin{aligned}
f(x) = f_p(x) &= x^{p-1} \prod_{k=1}^{m} (k-x)^p \\
&= a_{p-1}\, x^{p-1} + \ldots + a_n\, x^n \quad \in \mathbb{Z}[x] \qquad (2.2)
\end{aligned}$$

mit $a_{p-1} = (m!)^p$, $n = (m+1)\, p - 1$. Da die Zahlen $1, \ldots, m$ p–fache Nullstellen sind, kann f zugleich als

$$f(x) = a_{p,k}(x-k)^p + \ldots + a_{n,k}(x-k)^n \quad (a_{\nu,k} \in \mathbb{Z};\ k = 1, \ldots m) \tag{2.3}$$

geschrieben werden.

3. Auf f werde der Hilfssatz angewandt. Nach Annahme 1. ist

$$\begin{aligned}
0 = F(0)\, g(e) &= \sum_{j=0}^{m} b_j\, F(0)\, e^j \\
&= \sum_{j=0}^{m} b_j\, F(j) + \sum_{j=0}^{m} b_j\, G(j).
\end{aligned}$$

4. Nach Definition von F, (2.2) und (2.3) gilt

$$\begin{aligned} A_p &\underset{\text{Df}}{=} \sum_{j=0}^{m} b_j \; F(j) \\ &= b_0 \sum_{\mu=0}^{n} f^{(\mu)}(0) + \sum_{j=1}^{m} b_j \; \sum_{\mu=0}^{n} f^{(\mu)}(j) \\ &= b_0\big((m!)^p(p-1)! + a_p \; p! + \ldots + a_n \; n!\big) + \sum_{j=1}^{m} b_j(a_{p,j} \; p! + \ldots + a_{n,j} \; n!) \\ &= b_0(m!)^p \; (p-1)! + a'p! \quad (a' \in \mathbb{Z}). \end{aligned}$$

Da $b_0(m!)^p$ nach (2.1) nicht durch p teilbar ist, ist A_p eine durch $(p-1)!$, aber nicht durch p teilbare Zahl, also

$$|A_p| = \big|\sum_{j=0}^{m} b_j \; F(j)\big| \geq (p-1)! \tag{4.1}$$

5. Nach 3. und dem Hilfssatz ist

$$|A_p| = \big|\sum_{j=0}^{m} b_j \; G(j)\big| \leq \sum_{j=0}^{m} |b_j| \; e^j \sum_{\nu=p-1}^{n} |a_\nu| \; j^\nu.$$

Die innere Summe läßt sich nach (2.2) abschätzen durch $j^{p-1} \sum_{k=1}^{m}(k+j)^p \leq (2m^2)^p$, also

$$|A_p| \leq (2m^2)^p \; e^m \sum_{j=0}^{m} |b_j| = C_1 C_2^p. \tag{5.1}$$

C_1 und C_2 hängen von m und den b_j, aber nicht von p ab.

6. (4.1) und (5.1) sind für hinreichend großes p nicht miteinander verträglich, da

$$(p-1)! \geq \big(\frac{p}{3}\big)^{p/2} > C_1 C_2^p.$$

Die Annahme in 1. war also falsch, e ist transzendent. □

Im Beweis zu π wird mehrfach mit dem aus der Algebra bekannten Satz über symmetrische Polynome argumentiert. Der Vollständigkeit halber soll dieser hier kurz dargestellt werden.

3.7. Def.

(1) Ein Polynom $f(x_1, \ldots, x_n) \in R[x_1, \ldots, x_n]$ heißt **symmetrisch**, wenn für jede n–Permutation σ das Polynom $f\big(x_{\sigma(1)}, \ldots, x_{\sigma(n)}\big)$ mit f übereinstimmt.

Bsp. $f(x_1, x_2, x_3) = x_1^3x_2 + x_1^3x_3 + x_1x_2^3 + x_1x_3^3 + x_2^3x_3 + x_2x_3^3$ ist symmetrisch.
$g(x_1, x_2) = x_1^2x_2 + 2x_1x_2^2$ ist es nicht, da g durch Vertauschung von x_1 und x_2 in $x_1x_2^2 + 2x_1^2x_2 \neq g$ übergeht.

(2) Die speziellen symmetrischen Polynome

$$\begin{aligned}
\sigma_1 = \sigma_1(x_1, \ldots, x_n) &= x_1 + \ldots + x_n \\
\sigma_2 = \sigma_2(x_1, \ldots, x_n) &= \sum_{1 \leq \nu_1 < \nu_2 \leq n} x_{\nu_1}\, x_{\nu_2} \\
&\vdots \\
\sigma_n = \sigma_n(x_1, \ldots, x_n) &= x_1 \cdot \ldots \cdot x_n
\end{aligned}$$

(σ_k : Summe aller Produkte aus k verschiedenen Unbestimmten) heißen **die elementarsymmetrischen Funktionen** (in den Unbestimmten $x_1, \ldots, x_n$).

3.8. Hauptsatz über symmetrische Polynome. Jedes symmetrische $f(x_1, \ldots, x_n) \in R[x_1, \ldots, x_n]$ läßt sich schreiben als Polynom in $\sigma_1, \ldots, \sigma_n$ mit Koeffizienten in R.

Beweis:
1. f ist Summe von Termen $a\, x_1^{\alpha_1} \cdots x_n^{\alpha_n}$ $(a \in R, \alpha_j \in \mathbb{N}_0)$. Die Exponenten– n–Tupel $(\alpha_1, \ldots, \alpha_n)$ werden wie folgt – lexikografisch – angeordnet.

$(\alpha_1, \ldots, \alpha_n)$ steht vor $(\beta_1, \ldots, \beta_n) \neq (\alpha_1, \ldots, \alpha_n)$, wenn

a) $\alpha_1 + \ldots + \alpha_n > \beta_1 + \ldots + \beta_n$ oder

b) $\alpha_1 + \ldots + \alpha_n = \beta_1 + \ldots + \beta_n$ und ein $k, 0 \leq k \leq n-1$ existiert mit $\alpha_1 = \beta_1, \ldots, \alpha_k = \beta_k$ und $\alpha_{k+1} > \beta_{k+1}$.

2. Im symmetrischen f seien die Terme lexikographisch angeordnet. Für den ersten Term $a\, x_1^{\alpha_1} \cdots x_n^{\alpha_n}$ gilt $\alpha_1 \geq \ldots \geq \alpha_n$, denn in f tritt auch jeder andere auf, der durch Umordnen der α_j entsteht. Man bilde

$$f_1 = f - a\, \sigma_1^{\alpha_1 - \alpha_2}\, \sigma_2^{\alpha_2 - \alpha_3} \ldots\, \sigma_{n-1}^{\alpha_{n-1} - \alpha_n}\, \sigma_n^{\alpha_n}.$$

f_1 ist symmetrisch. Der erste Term des σ–Ausdrucks ist

$$\begin{aligned}
&= a\, x_1^{\alpha_1 - \alpha_2} (x_1x_2)^{\alpha_2 - \alpha_3} \ldots (x_1 \ldots x_n)^{\alpha_n} \\
&= a\, x_1^{\alpha_1} \ldots x_n^{\alpha_n}.
\end{aligned}$$

f_1 besteht also nur aus Termen, die $x_1^{\alpha_1} \cdots x_n^{\alpha_n}$ nachfolgen. Es gibt nur endlich viele n–Tupel $(\beta_1, \ldots, \beta_n)$ nach $(\alpha_1, \ldots, \alpha_n)$. Es reichen also endlich viele der obigen Schritte, so daß die Differenz schließlich das Nullpolynom ist. $\square$

Ein **Beispiel**:

$$\begin{aligned} f(x_1,x_2) &= x_1^3x_2 + x_1x_2^3 \in \mathbb{Z}[x_1,x_2], \\ f_1(x_1,x_2) &= f(x_1,x_2) - \sigma_1^{3-1}\ \sigma_2 = f(x_1,x_2) - (x_1+x_2)^2\ x_1x_2 \\ &= -2x_1^2\ x_2^2 = -2\sigma_2^2, \end{aligned}$$

also

$$f(x_1,x_2) = \sigma_1^2\sigma_2 - 2\sigma_2^2.$$

Die praktische Durchführung ist im allgemeinen recht mühsam.

Ist z.B. $f(x) = x^n + a_{n-1}\ x^{n-1} + \ldots + a_0 \quad \in \mathbb{Z}[x]$ und $f(x) = (x-\alpha_1)\ldots(x-\alpha_n)$, dann folgt

$$f(x) = x^n - \sigma_1(\alpha_1,\ldots,\alpha_n)\ x^{n-1} + \sigma_2(\ )\ x^{n-2} - + \ldots + (-1)^n\ \sigma_n(\ ).$$

D.h. die elementarsymmetrischen Funktionen der Nullstellen $\alpha_1,\ldots,\alpha_n$ liegen in $\mathbb{Z}$ (ebenso mit $\mathbb{Q}$ statt $\mathbb{Z}$).

Nach diesem Prinzip wird der Beweis geführt, daß mit α und β auch $\alpha+\beta$ und $\alpha\cdot\beta$ algebraisch sind. Er werde für $\alpha+\beta$ ausgeführt. Seien

$$\begin{aligned} f(x) &= x^n + a_{n-1}\ x^{n-1} + \ldots + a_0 \quad \in \mathbb{Q}[x], \\ g(x) &= x^m + b_{m-1}\ x^{m-1} + \ldots + b_0 \quad \in \mathbb{Q}[x] \end{aligned}$$

die Minimalpolynome zu α bzw. β.
Seien $\alpha = \alpha_1,\alpha_2,\ldots,\alpha_n$ und $\beta = \beta_1,\beta_2,\ldots,\beta_m$ die jeweiligen Konjugierten.
Man bilde

$$h(x) = \prod_{j=1,\ldots,n;k=1,\ldots,m} \big(x - (\alpha_j+\beta_k)\big) \quad \in \mathbb{Q}[x,\alpha_1,\ldots,\alpha_n,\beta_1,\ldots,\beta_m].$$

Ersetzt man $\alpha_1,\ldots,\alpha_n,\beta_1,\ldots,\beta_m$ durch Unbestimmte $y_1,\ldots,y_n,\ z_1,\ldots,z_m,$ dann entsteht ein Polynom $h_1(x,y,z) \in \mathbb{Q}[x,y,z]$. Dies kann auch als Polynom $h_2 \in \mathbb{Q}[x,y_1,\ldots,y_n]\ [z_1,\ldots,z_m]$ (in den Variablen $z_1\ldots,z_m$ mit Koeffizienten aus $\mathbb{Q}[x,y_1,\ldots,y_m]$) aufgefaßt werden. h_2 ist symmetrisch in $z_1,\ldots,z_m$. Da die elementarsymmetrischen Funktionen von $z_1,\ldots,z_m,$ mit z_j ersetzt durch β_j, aus $\mathbb{Q}$ stammen, ist

$$h_2(\beta_1,\ldots,\beta_m) \in \mathbb{Q}[x,y_1,\ldots,y_n]$$

und symmetrisch in $y_1,\ldots,y_n$. Die gleiche Schlußweise mit den $\sigma_1,\ldots,\sigma_n$ in $\alpha_1,\ldots,\alpha_n$ zeigt, daß $h(x)$ Koeffizienten in $\mathbb{Q}$ hat.

$\alpha_1 + \beta_1 = \alpha + \beta$, als Nullstelle von h, ist somit algebraisch. Genauso verfährt man mit $\alpha \cdot \beta$. Daß mit α auch α^{-1} (falls $\alpha \neq 0$) algebraisch ist, sieht man unmittelbar.

Es dauerte nahezu zehn Jahre nach Hermite's Beweis, bis Ferdinand Lindemann 1882 in Freiburg die Argumentation auf π übertragen konnte. Der Beweis der Transzendenz von π ist insofern bedeutsam, als damit die Frage nach der Quadratur des Kreises negativ beantwortet wird. Denn könnte man in endlich vielen Schritten mit Zirkel und Lineal aus dem Radius eines Kreises die Seitenlänge eines flächengleichen Quadrats konstruieren, müßte π algebraisch sein.

3.9. Satz von Lindemann (1882, Carl Louis Ferdinand von L., 1852–1939).
Die Zahl π ist transzendent.

Beweis.
1. Es werde angenommen, daß π algebraisch ist, dann nach 3.1.(7) auch $i\pi$. Nach 3.1.(4) existiert ein $d \in \mathbb{N}$, so daß $di\pi$ ganz–algebraisch ist. Sei

$$g(x) = x^m + b_{m-1}\, x^{m-1} + \ldots + b_0 \in \mathbb{Z}[x] \tag{1.1}$$

ein Polynom mit $di\pi$ als Nullstelle. g zerfalle wie folgt

$$g(x) = \prod_{j=1}^{m} (x - d\alpha_j), \quad \alpha_1 = i\pi. \tag{1.2}$$

Wegen $0 = 1 + e^{i\pi} = e^0 + e^{\alpha_1}$ gilt

$$R \underset{\text{Df}}{=} \prod_{j=1}^{m} \left(e^0 + e^{\alpha_j}\right) = 0. \tag{1.3}$$

2. Das Produkt R werde ausmultipliziert und als

$$R = k + e^{\beta_1} + \ldots + e^{\beta_\ell}$$

geschrieben. Dabei sind die β_ν die nicht verschwindenden (nicht notwendig verschiedenen) unter den Zahlen

$$\varepsilon_1\alpha_1 + \ldots + \varepsilon_m\alpha_m, \quad \varepsilon_\nu \in \{0, 1\}. \tag{2.1}$$

$k = 2^m - \ell \geq 1$ ist die Anzahl der verschwindenden Summen (2.1).

3. Für primes, später hinreichend groß zu wählendes

$$p > \max\left(k, d, \prod_{\nu=1}^{\ell} d|\beta_\nu|\right) \tag{3.1}$$

werde

$$f(x) = f_p(x) = (dx)^{p-1} \prod_{\nu=1}^{\ell} \big(dx - d\beta_\nu\big)^p \tag{3.2}$$
$$= a_{p-1}\, x^{p-1} + \ldots + a_n\, x^n \qquad \big(n = (\ell+1)p - 1\big)$$

gesetzt. Die Schreibweise deutet an, daß die a_ν aus $\mathbb{Z}$ stammen. Zum Beweis hierfür bedenke man, daß die a_ν symmetrisch sind in $d\beta_1, \ldots, d\beta_\ell$ (genauer: in Unbestimmten, die man an die Stellen der $d\beta_\nu$ setzt). Die elementarsymmetrischen Funktionen (esF) in $d\beta_1, \ldots, d\beta_\ell$ sind gleich den esF in den d–Fachen der 2^m Summen (2.1). (Denn setzt man z.B. in $\sigma_j(x_1, \ldots, x_r)\ x_1 = \ldots = x_j = 0,$ dann bleiben die esF in $x_{j+1}, \ldots x_r$). Die esF in den Summen (2.1) sind symmetrisch in $d\alpha_1, \ldots, d\alpha_m$. Die esF hiervon sind wegen (1.2) aus $\mathbb{Z}$. Mehrfache Anwendung von 3.8. ergibt $f(x) \in \mathbb{Z}[x]$. (3.1) bedingt

$$p \nmid a_{p-1}. \tag{3.3}$$

4. Für $\nu = 1, \ldots, \ell$ kann

$$f(x) = \gamma_{p,\nu}(x - \beta_\nu)^p + \ldots + \gamma_{n,\nu}(x - \beta_\nu)^n \tag{4.1}$$

geschrieben werden. Für $p \le \mu \le n$ ist

$$\sum_{\nu=1}^{\ell} \gamma_{\mu,\nu} = a'_\mu \in \mathbb{Z}. \tag{4.2}$$

Denn die Summe läßt sich darstellen als

$$\frac{1}{\mu!} \sum_{\nu=1}^{\ell} f^{(\mu)}(\beta_\nu) \quad \big(f^{(\mu)}(\beta_\nu) = \mu!\ \gamma_{\mu,\nu}\big).$$

Nach Definition von f ist dies ein in $d\beta_1, \ldots, d\beta_\ell$ symmetrisches Polynom mit Koeffizienten in $\mathbb{Z}$.

5. Ähnlich wie im Beweis zu Satz 3.5. mit dem obigen f und (1.3) ergibt sich

$$0 = F(0)R = F(0)\Big(k + \sum_{\nu=1}^{\ell} e^{\beta_\nu}\Big)$$
$$= k\ F(0) + \sum_{\nu=1}^{\ell} F(\beta_\nu) + \sum_{\nu=1}^{\ell} G(\beta_\nu) \tag{5.1}$$
$$\big(F(x) = \sum_{\mu=0}^{n} f^{(\mu)}(x), \quad G(x) = F(0)e^x - F(x)\big).$$

Nach (3.1), (3.2) und (3.3) ist

$$\begin{aligned} k\ F(0) &= k(p-1)!\ \big(a_{p-1} + p\ a_p + \ldots + \frac{n!}{(p-1)!}a_n\big) \\ &\equiv 0\big((p-1)!\big), \quad \text{aber} \quad \not\equiv 0(p). \end{aligned}$$

Aus (4.1) und (4.2) folgt

$$\begin{aligned} \sum_{\nu=1}^{\ell} F(\beta_\nu) &= \sum_{\nu=1}^{\ell}\ \sum_{\mu=0}^{\nu}\ f^{(\mu)} = \sum_{\nu=1}^{\ell}\ \sum_{\mu=p}^{n}\ \mu!\ \gamma_{\mu,\nu} \\ &= \sum_{\mu=p}^{n} \mu!\, a'_\mu \equiv \mathrm{O}(p!). \end{aligned}$$

Zusammenfassung mit (5.1) zeigt, daß $\sum_{\nu=l}^{\ell} G(\beta_\nu)$ eine ganze, durch $(p-1)!$, aber nicht durch p teilbare Zahl ist, d.h.

$$\Big|\sum_{\nu=1}^{\ell} G(\beta_\nu)\Big| \geq (p-1)!\ . \tag{5.2}$$

6. Bei der umgekehrten Abschätzung mit Hilfssatz 3.6. kann man wieder relativ großzügig vorgehen.

$$\begin{aligned} \Big|\sum_{\nu=1}^{\ell} G(\beta_\nu)\Big| &\leq \sum_{\nu=1}^{\ell} e^{|\beta_\nu|}\ \sum_{j=p-1}^{n}\ |a_j|\ \ |\beta_\nu|^j \\ &\leq \sum_{\nu=1}^{\ell}\ e^{|\beta_\nu|}\big(d|\beta_\nu|\big)^{p-1}\Big(\prod_{\mu=1}^{\ell}\big(d|\beta_\nu| + d|\beta_\mu|\big)^p\Big) \\ &\leq C^p, \end{aligned}$$

wobei C von d, ℓ und den β_ν abhängen kann, aber nicht von p.

Das stärkere Wachstum von $(p-1)!$ gegenüber C^p führt bei hinreichend großem p auf einen Widerspruch zu (5.2). Also war die Annahme, π sei algebraisch, falsch. □

4. Kapitel. Primzahlen in Restklassen

Literatur: J. Brüdern. Einführung in die analytische Zahlentheorie

p und q bezeichnen stets Primzahlen.

Am Beispiel der Darstellbarkeit einer natürlichen Zahl als Summe zweier Quadrate ($p \equiv 1$ oder 3 mod 4) oder des zweiten Ergänzungsgesetzes zum quadratischen Reziprozitätsgesetz ($p \equiv 1, 3, 5$ oder 7 mod 8) sieht man, daß es wichtig ist, über die Verteilung der Primzahlen in den Restklassen mod m ($m \in \mathbb{N}$ ein fester Modul) Bescheid zu wissen. Dabei braucht man offenbar nur die reduzierten Restklassen mod m zu betrachten. Denn ist $d = (a, m) > 1$ und $p \equiv a(m)$, dann folgt $d|p$. In einer nicht reduzierten Restklasse liegt daher höchstens eine Primzahl. Der Euklidsche Beweis zur Unendlichkeit der Primzahlmenge läßt sich nur auf ganz spezielle Restklassen übertragen. 1837 bewies Dirichlet die lange vermutete Aussage, daß jede reduzierte Restklasse $a \bmod m$ unendlich viele Primzahlen enthält. Im Zuge des Beweises zum Primzahlsatz konnte man zeigen, daß die Primzahlen in den $\varphi(m)$ reduzierten Restklassen mod m asymptotisch gleichmäßig verteilt sind (Primzahlsatz in Progressionen). Dirichlet führte seinen Beweis mittels der von ihm eingeführten Charaktere, die es erlauben, die Bedingung $p \equiv a(m)$ in günstiger Weise umzuformulieren.

4.1. Satz und Def. (Dirichlet).
Zu jedem $m \in \mathbb{N}$ existieren genau $\varphi(m)$ (= Euler–Funktion) Funktionen $\chi : \mathbb{Z} \to \mathbb{C}$ mit

(1) $\chi(a) = 0$ für alle $(a, m) > 1$,

(2) $|\chi(a)| = 1$ für alle $(a, m) = 1$,

(3) $\chi(a_1 a_2) = \chi(a_1)\, \chi(a_2)$ für alle a_1, a_2,

(4) $\chi(a + m) = \chi(a)$ für alle a.

((3) besagt, daß die χ vollständig multiplikativ sind, (4) bedeutet Periodizität mod m.)

Jede solche Funktion heißt ein **(Restklassen-** oder **Dirichlet-) Charakter** mod m. Der Charakter χ_0 mit $\chi_0(a) = 1$ für $(a, m) = 1$ heißt der **Hauptcharakter** mod$m$.

Beweis.
1. Die Konstruktion soll der Einfachheit halber zuerst im Fall

$$m = p_1^{k_1} \dots p_\ell^{k_\ell} \quad \text{mit} \quad 2 < p_1 < \dots < p_\ell$$

vorgestellt werden. Zu jedem $m_j \underset{\text{Df}}{=} p_j^{k_j}$ $(1 \le j \le \ell)$ sei g_j eine Primitivwurzel, d.h. $\{1 = g_j^0, g_j, \ldots, g_j^{\varphi(m_j)-1}\}$ bildet ein primes Restsystem mod m_j.
Ist $(a, m) = 1$, so existieren eindeutig $b_1, \ldots, b_\ell$ mit $0 \le b_j \le \varphi(m_j) - 1$, so daß

$$a \equiv g_j^{b_j} \mod m_j \quad (j = 1, \ldots, \ell).$$

Man nennt $(b_1, \ldots, b_\ell)$ das **Index–System** (IS) von a mod m. Multiplikation zweier zu m primer a und a' entspricht Addition der IS, wobei in jeder Komponente mod $\varphi(m_j)$ reduziert wird.
Die obige Feststellung kann so ausgedrückt werden, daß $\mathbb{Z}_m^*$ das direkte Produkt der zyklischen Gruppen $\mathbb{Z}_{\varphi(m_j)}$ ist.

$$\mathbb{Z}_m^* \cong \mathbb{Z}_{\varphi(m_1)} \times \ldots \times \mathbb{Z}_{\varphi(m_\ell)}.$$

2. Sei ξ ein Homomorphismus von $\mathbb{Z}_m^*$ in $(\mathbb{C}\backslash\{0\}, \cdot\,)$, d.h. $\xi(a_1 a_2) = \xi(a_1)\,\xi(a_2)$. Ist für $1 \le j \le \ell$ a_j so gewählt, daß

$$a_j \equiv g_j(m_j), \quad a_j \equiv 1(m_r) \quad \text{für} \quad 1 \le r \le \ell, \quad r \ne j,$$

und gehört zu $a \in \mathbb{Z}_m^*$ das IS $(b_1, \ldots, b_\ell)$, so gilt

$$\xi(a) = \big(\xi(a_1)\big)^{b_1} \ldots \big(\xi(a_\ell)\big)^{b_\ell}.$$

ξ ist also durch die Vorgabe von $\xi(a_1), \ldots, \xi(a_\ell)$ vollständig festgelegt. Wegen $a_j^{\varphi(m_j)} \equiv 1\ (m)$ und $\xi(1) = 1$ gilt $\xi(a_j)^{\varphi(m_j)} = 1$. $\eta_j \underset{\text{Df}}{=} \xi(a_j)$ ist somit eine $\varphi(m_j)$–te Einheitswurzel. Umgekehrt kann für $\xi(a_j)$ jede solche Einheitswurzel genommen werden. Jedes ℓ–Tupel $(\eta_1, \ldots, \eta_\ell)$ von Einheitswurzeln definiert somit ein ξ. Verschiedenen Tupeln entsprechen verschiedene ξ. Also lassen sich genau $\varphi(m_1) \cdot \ldots \cdot \varphi(m_\ell) = \varphi(m)$ Homomorphismen ξ angeben.

Die Konstruktion zeigt auch, daß die ξ mit der Multiplikation als Verknüpfung eine zu $\mathbb{Z}_m^*$ isomorphe Gruppe bilden.

3. Sei ξ ein Homomorphismus wie in 2. Durch

$$\chi(a) \underset{\text{Df}}{=} \begin{cases} 0, & \text{falls} \quad (a, m) > 1, \\ \xi(a + m\mathbb{Z}), & \text{falls} \quad (a, m) = 1 \end{cases}$$

wird ein Charakter definiert. Es ist nur noch Eigenschaft (3) im Fall $(a_1 a_2, m) = 1$ nachzuweisen. Hier hat man

$$\begin{aligned} \chi(a_1)\,\chi(a_2) &= \xi(a_1 + m\mathbb{Z})\,\xi(a_2 + m\mathbb{Z}) \\ &= \xi\big((a_1 + m\mathbb{Z})\,(a_2 + m\mathbb{Z})\big) = \xi(a_1 a_2 + m\mathbb{Z}) = \chi(a_1 a_2). \end{aligned}$$

Umgekehrt definiert jeder Charakter χ einen Homomorphismus. Daher ist die Anzahl $= \varphi(m)$.

4. Mit χ_1 und χ_2 sind $\chi_1\chi_2$ und $\overline{\chi}_1$ Charaktere. Ist χ fest, und durchläuft χ' alle Charaktere, dann auch $\chi\chi'$. Dies sieht man mit der Gruppen–Eigenschaft der Homomorphismen. Der Hauptcharakter spielt offenbar die Rolle des neutralen Elements. Wegen $\chi\overline{\chi} = \chi_0$ kann $\overline{\chi}$ als „zu χ inverser Charakter“ angesehen werden.

5. Im Fall

$$m = 1, 2, 4 \quad \text{bzw.} \quad m = \left(2p_1^{k_1}\right) p_2^{k_2} \dots p_\ell^{k_\ell} \quad (2 < p_1 < \dots < p_\ell)$$

kann man wie oben vorgehen.
Im Fall

$$m = 2^{k_0}\, p_1^{k_1} \dots p_\ell^{k_\ell} \quad (\ell \geq 1,\ k_0 \geq 2) \quad \text{bzw.} \quad m = 2^{k_0} \quad (k_0 \geq 3)$$

benutzt man die Darstellung der primen Reste $\bmod 2^{k_0}$ durch $(-1)^b\, 5^{b'}$ $(b = 0, 1;\ 0 \leq b' < 2^{k-2})$. Hier ist das Index–System um eine Komponente länger. Die übrigen Überlegungen verlaufen wie oben. □

Beispiele.
1. Zu $m = 5$ gehört die Primitivwurzel 2, also

$$\mathbb{Z}_5^* = \{1(\equiv 2^0),\ 2(\equiv 2^1),\ 3(\equiv 2^3),\ 4(\equiv 2^2)\}.$$

Die vierten Einheitswurzeln $1, i, -1, -i$ ergeben die vier Charaktere

	0	1	2	3	4
χ_0	0	1	1	1	1
χ_1	0	1	i	$-i$	-1
χ_2	0	1	-1	-1	1
χ_3	0	1	$-i$	i	-1.

2. Wegen $\mathbb{Z}_{12}^* \cong \mathbb{Z}_4^* \times \mathbb{Z}_3^*$, $\mathbb{Z}_4^* = \{1(\equiv 3^0), 3(\equiv 3^1)\}$, $\mathbb{Z}_3^* = \{1(\equiv 2^0), 2(\equiv 2^1)\}$
haben die Elemente von $\mathbb{Z}_{12}^*$ die ISe

$$1 : (0,0), \quad 5 : (0,1), \quad 7 : (1,0), \quad 11 : (1,1).$$

Mit den jeweils zwei Einheitswurzeln $1, -1$ ergibt dies mod 12 die vier Charaktere (nur für $(a, 12) = 1$ angegeben)

(η_1,η_2)		1	5	7	11
(1,1)	χ_0	1	1	1	1
(-1,1)	χ_1	1	1	-1	-1
(1,-1)	χ_2	1	-1	1	-1
(-1,-1)	χ_3	1	-1	-1	1.

3. Für $p > 2$ wird durch

$$\chi(a) = \begin{cases} 0, & (a,p) > 1 \\ \left(\frac{a}{p}\right), & (a,p) = 1 \quad \text{(Legendre–Symbol)} \end{cases}$$

ein reeller, vom Hauptcharakter χ_0 verschiedener Charakter mod p definiert.

Für $m \in \mathbb{N}$ bedeute $\sum_{\chi \bmod m}$ (bzw. $\sum_{\chi}$, wenn klar ist, um welchen Modul es sich handelt) Summation über alle $\varphi(m)$ Charaktere mod m. $\sum_a^*$ bedeute Summation über ein primes Restsystem mod m. Die letzte Vereinbarung ist nur sinnvoll, wenn das Summengewicht m–periodisch ist.

Die Beispiele legen nahe, daß in der „Charakter–Matrix“ Summation über eine Zeile oder eine Spalte entweder $\varphi(m)$ oder Null ergibt. Dies ist allgemein so.

4.2. Hilfssatz (Orthogonalitätsrelationen für Charaktere).
Sei χ_1 ein Charakter mod m, $(b,m) = 1$. Dann gilt

$$(1) \qquad \sum_a^* \chi_1(a) = \begin{cases} \varphi(m), & \text{falls} \quad \chi_1 = \chi_0, \\ 0 & \text{sonst.} \end{cases}$$

$$(2) \qquad \sum_\chi^* \chi(b) = \begin{cases} \varphi(m), & \text{falls} \quad b \equiv 1(m), \\ 0 & \text{sonst.} \end{cases}$$

Beweis zu (1). Für $\chi_1 = \chi_0$ ist nichts zu zeigen. Im Fall $\chi_1 \neq \chi_0$ gibt es ein g mit $(g,m) = 1$ und $\chi_1(g) \neq 1$. Da mit a auch ga ein reduziertes Restsystem mod m durchläuft, folgt mit den Eigenschaften (4) und (3) von χ_1

$$\sum_a^* \chi_1(a) = \sum_a^* \chi_1(ga) = \chi_1(g) \sum_a^* \chi_1(a).$$

Dies gilt nur, wenn die Summe verschwindet.

Zu (2). Für $m = p_1^{k_1} \dots p_\ell^{k_\ell}$, $2 < p_1 < \dots < p_\ell$, $b \not\equiv 1(m)$ sei im Sinn des Beweises zu Satz 4.1. $(b_1, \dots, b_\ell)$ das IS zu b. Hierin ist mindestens ein $b_j \neq 0$, oBdA b_1. Man konstruiert ein $\chi_1 \neq \chi_0$ über einen Homomorphismus ξ_1 mit den Einheitswurzeln

$$\eta_1 = \exp\left(2\pi i/\varphi(m_1)\right), \quad \eta_2 = \dots = \eta_\ell = 1.$$

Dies ergibt

$$\chi_1(b) = \xi_1(b + m\mathbb{Z}) = \eta_1^{b_1} \neq 1.$$

Da mit χ auch $\chi\chi_1$ alle Charaktere mod m durchläuft, gilt

$$\sum_\chi \chi(b) = \sum_\chi (\chi\chi_1)(b) = \chi_1(b) \sum_\chi \chi(b),$$

woraus die Behauptung folgt. Für $2|m$ wird ähnlich argumentiert. □

Die nächste Formel enthält das angekündigte Verfahren, Summen mit Restklassenbedingungen durch glatte Summen zu ersetzen.

4.3. Satz. Sei $f : \mathbb{N} \to \mathbb{C}, \quad \sum_k |f(k)| < \infty, \ (a, m) = 1.$
Dann gilt

$$\sum_{k, k\equiv a(m)} f(k) = \frac{1}{\varphi(m)} \sum_\chi \overline{\chi}(a) \ \sum_k f(k) \ \chi(k).$$

Beweis. Sei $aa^* \equiv 1(m)$. Dann ist für jedes χ mod m

$$1 = \chi(1) = \chi(aa^*) = \chi(a) \ \chi(a^*),$$

also $\overline{\chi}(a) = \chi(a^*)$. Für $(k, m) = 1$ sieht man daraus mit 4.2.(2)

$$\begin{aligned} \frac{1}{\varphi(m)} \sum_\chi \overline{\chi}(a) \ \chi(k) &= \frac{1}{\varphi(m)} \sum_\chi \chi(a^* k) \\ &= \begin{cases} 1, & \text{falls } \ a^*k \equiv 1(m) \\ 0 & \text{sonst} \end{cases} = \begin{cases} 1, & \text{falls } \ k \equiv a(m) \\ 0 & \text{sonst.} \end{cases} \end{aligned}$$

Da in der k–Summe auf der rechten Seite in 4.3. die nicht zu m teilerfremden k mit $\chi(k) = 0$ bewichtet werden, folgt die Behauptung. □

4.4. Hilfssatz. Für $\chi \neq \chi_0 \bmod m, \quad 0 < A < B$ gilt

$$\Big| \sum_{A<k\leq B} \chi(k) \Big| \leq \varphi(m).$$

Beweis. Das Intervall $(A, B]$ wird in Teile mit einer vollen Periode mod m und ein Reststück zerlegt. Die Perioden bringen nach 4.2.(1) den Beitrag Null, das Letztere bringt höchstens $\varphi(m)$ Summanden vom Betrag Eins. □

Beim analytischen Zugang zu den Primzahlen in Restklassen erweisen sich, ähnlich wie die Zeta–Funktion beim Primzahlsatz, die Dirichlet–Reihen zu den Charakteren als nützlich.

4.5. Def. und Satz.

(1) Für einen Charakter χ mod m heißt die (für $\sigma = \text{Re } s > 1$ absolut konvergente) Reihe

$$L(s,\chi) = \sum_{n=1}^{\infty} \chi(n)\ n^{-s}$$

die **Dirichletsche** L**–Reihe** (oder L**–Funktion**) zum Charakter χ.

(2) $L(s,\chi_0) = \zeta(s).\prod_{p|m}\big(1-\frac{1}{p^s}\big)$.

Insbesondere ist $L(s,\chi_0)$ bis auf einen Pol erster Ordnung bei $s=1$ mit dem Residuum $\varphi(m)/m$ in die Halbebene $\{s,\sigma>0\}$ analytisch fortsetzbar. $L(s,\chi_0)$ hat dort dieselben Nullstellen wie $\zeta(s)$.

(3) Für $\chi \neq \chi_0$ ist die Reihe $L(s,\chi)$ in $\{s,\sigma>0\}$ kompakt gleichmäßig konvergent und stellt dort eine holomorphe Funktion dar.

Beweis.

1. Wegen $|\chi(n)| \leq 1$ liegt wie bei $\zeta(s)$ für $\sigma > 1$ absolute Konvergenz und Holomorphie der L–Reihen vor.

2. Zu (2). Aus der elementaren Zahlentheorie ist bekannt, wie in einer Summe eine Teilerfremdheitsbedingung aufgelöst werden kann.
Mit

$$\varepsilon(k) = \sum_{d|k}\mu(d) = \begin{cases} 1, & k=1 \\ 0 & \text{sonst} \end{cases}$$

folgt für $f:\mathbb{N}\to\mathbb{C}$ mit absolut konvergenter Summe $\sum_n f(n)$

$$\begin{aligned}\sum_{n,(n,m)=1} f(n) &= \sum_n f(n) \sum_{d|(n,m)}\mu(d) \\ &= \sum_{d|m}\mu(d) \sum_{n,n\equiv 0(d)} f(n).\end{aligned}$$

Für $\sigma > 1$ gilt daher

$$\begin{aligned}L(s,\chi_0) &= \sum_{n,(n,m)=1} n^{-s} = \sum_{d|m}\mu(d) \sum_{n,n\equiv 0(d)} n^{-s} \\ &= \sum_{d|m}\mu(d)\ d^{-s}\zeta(s) = \zeta(s)\prod_{p|m}\big(1-p^{-s}\big).\end{aligned}$$

Aus der Fortsetzbarkeit der ζ–Funktion ergeben sich die übrigen Eigenschaften. Der Faktor $\prod_{p|m}\big(1-p^{-s}\big)$ hat für $\sigma>0$ keine Nullstelle.

3. Für $\chi\neq\chi_0,\quad 0<A<B$ ergibt sich mit partieller Summation

$$\sum_{A<n\le B}\chi(n)\;n^{-s}=B^{-s}\sum_{A<n\le B}\chi(n)+s\int_A^B\Big(\sum_{A<n\le x}\chi(n)\Big)\;x^{-s-1}\;dx.$$

4.4. bewirkt

$$\begin{aligned}\Big|\sum_{A<n\le B}\chi(n)\;n^{-s}\Big|&\le\varphi(m)\big(B^{-\sigma}+|s|\int_A^B x^{-\sigma-1}\;dx\big)\\&<\varphi(m)\Big(1+\frac{|s|}{\sigma}\Big)A^{-\sigma}.\end{aligned}$$

Hieraus folgt leicht die kompakt gleichmäßige Konvergenz für $\sigma>0$. □

4.6. Hilfssatz. Für $\sigma>1$ gilt

(1) $\sum_n\mu(n)\;\chi(n)\;n^{-s}=1/L(s,\chi)$, insbesondere ist dort $L(s,\chi)\neq0$,

(2) $\sum_n\Lambda(n)\;\chi(n)\;n^{-s}=-\dfrac{L'}{L}(s,\chi)$,

(3) $\sum_{n\equiv a(m)}\Lambda(n)\;n^{-s}=-\dfrac{1}{\varphi(m)}\sum_{\chi\bmod m}\overline{\chi}(a)\;\dfrac{L'}{L}(s,\chi)$ (falls $(a,m)=1$).

Beweis. Die Herleitung verläuft wie bei $\zeta(s)$ mit dem Produktsatz, etwa zu (1).

$$\begin{aligned}L(s,\chi)\sum_n\mu(n)\;\chi(n)\;n^{-s}&=\sum_{k,n\in\mathbb{N}}\chi(k)\;\chi(n)\;\mu(n)\;(kn)^{-s}\\&=\sum_{r\in\mathbb{N}}r^{-s}\;\chi(r)\sum_{n|r}\mu(n)=1.\end{aligned}$$

Immer wieder wird die vollständige Multiplikativität der χ benutzt.
(3) ergibt sich mit Satz 4.3. und (2)

$$\sum_{n\equiv a(m)}\Lambda(n)\;n^{-s}=\frac{1}{\varphi(m)}\sum_\chi\overline{\chi}(a)\;\sum_n\Lambda(n)\;\chi(n)\;n^{-s}.$$

□

Ziel ist der Beweis einer asymptotischen Formel für $\pi(x,m,a)=\#\{p\le x,\;p\equiv a(m)\}$ im Fall $(m,a)=1$ (Satz 4.8). Es kann wie bei der Herleitung des Primzahlsatzes

vorgegangen werden. Zur Anwendung des Newman'schen Tauber–Satzes auf die Reihe $\sum_{n\equiv a(m)} \Lambda(n)\, n^{-s}$ ist wieder das analytische Verhalten auf der 1–Geraden und insbesondere das Nicht–Verschwinden der L–Reihen (außer für $\chi = \chi_0,\ \ s = 1$) zu untersuchen.

4.7. Satz (Dirichlet, Hadamard, de la Vallée–Poussin).
Für alle χ mod m und alle $t \in \mathbb{R}$ (außer $t = 0$ im Fall $\chi = \chi_0$) gilt

$$L(1 + it, \chi) \neq 0.$$

Vorbemerkung. Dirichlet bewies die schwächere Aussage $\sum_{p\equiv a(m)} \frac{1}{p} = \infty$. Hierzu reicht $L(1, \chi) \neq 0$ für $\chi \neq \chi_0$. Als kritisch erwiesen sich reellwertige Charaktere ungleich χ_0. Dirichlet nutzte hierzu aus, daß für solche χ $L(1, \chi)$ als Faktor in einer (nicht verschwindenden) Anzahl von Klassen quadratischer Formen auftritt und somit nicht verschwinden kann (s. hierzu D.B. Zagier, Zeta–Funktionen und quadratische Körper. Springer, 1981). Der hier angegebene Beweis verläuft direkt und geht auf Franz Carl Joseph Mertens (1840–1927) und Edmund Landau (1877–1938) zurück. Alle übrigen Fälle können nach der Idee von de la Vallée–Poussin behandelt werden.

Beweis.
1. Zu $L(1, \chi) \neq 0$ für $\chi \neq \chi_0,\ \chi^2 = \chi_0$.
1.1 Sei $f(n) = \sum_{d|n} \chi(d)$. f ist multiplikativ und liefert auf den Primzahlpotenzen die Werte

$$f(p^k) = \begin{cases} 1, & \text{falls} \quad p|m; \\ k+1, & \text{falls} \quad \chi(p) = 1; \\ 0, & \text{falls} \quad \chi(p) = -1 \quad \text{und} \quad k \quad \text{ungerade}; \\ 1, & \text{falls} \quad \chi(p) = -1 \quad \text{und} \quad k \quad \text{gerade} \end{cases}$$

Also ist stets $f(n) \geq 0$ und $f(n^2) \geq 1$.
Damit folgt

$$F(x) \underset{\text{Df}}{=} \sum_{n\leq x} f(n)\, n^{-1/2} \geq \sum_{r\leq x^{1/2}} r^{-1} \to \infty \quad \text{für} \quad x \to \infty. \tag{1.1}$$

1.2. Ähnlich wie bei der Untersuchung der Summe $\sum_{n\leq x} d(n)$ sieht man

$$F(x) = \sum_{n\leq x} n^{-1/2} \sum_{d|n} \chi(d) = \sum_{k,d,kd\leq x} \chi(d)\ (kd)^{-1/2}$$

$$= \sum_{d\leq x^{1/2}} \chi(d)\ d^{-1/2} \sum_{k\leq x/d} k^{-1/2} + \sum_{k\leq x^{1/2}} k^{-1/2} \sum_{x^{1/2}<d\leq x/k} \chi(d)\ d^{-1/2}. \tag{1.2.1}$$

Durch partielle Summation folgt

$$\sum_{k\le x/d} k^{-1/2} = \Big[\frac{x}{d}\Big]\ \Big(\frac{x}{d}\Big)^{-1/2} + \frac{1}{2}\ \int_1^{x/d} [t]\ t^{-3/2}\ dt$$

$$= \Big(\frac{x}{d}\Big)^{1/2} + O\Big(\Big(\frac{d}{x}\Big)^{1/2}\Big) + \frac{1}{2}\int_1^{x/d} t^{-1/2}\ dt - \frac{1}{2}\int_1^{x/d} (t-[t])\ t^{-3/2}\ dt$$

$$= 2\Big(\frac{x}{d}\Big)^{1/2} - C + O\Big(\Big(\frac{d}{x}\Big)^{1/2}\Big), \tag{1.2.2}$$

wobei

$$0 < C = 1 + \frac{1}{2}\int_1^{\infty} (t-[t])\ t^{-3/2}\ dt. \tag{1.2.3}$$

Mit Hilfssatz 4.4. und partieller Summation ergibt sich

$$\Big|\sum_{x^{1/2}<d\le x/k} \chi(d)\ d^{-1/2}\Big| \le 2m\ x^{-1/4}. \tag{1.2.4}$$

1.3. Zusammenfassung von (1.2.1),..., (1.2.4) liefert

$$F(x) = 2\ x^{1/2} \sum_{d\le x^{1/2}} \chi(d)\ d^{-1} - C \sum_{d\le x^{1/2}} \chi(d)\ d^{-1/2} + \mathrm{O}(1),$$

wobei die O–Konstante von m, aber nicht von x abhängen kann.

Für $N \ge x^{1/2}$ ergibt sich in ähnlicher Weise mit partieller Summation und Hilfssatz 1.4.

$$\sum_{x^{1/2}<d\le N} \chi(d)\ d^{-1} = \mathrm{O}\big(x^{-1/2}\big) \quad \text{und}$$

$$\sum_{x^{1/2}<d\le N} \chi(d)\ d^{-1/2} = \mathrm{O}\big(x^{-1/4}\big),$$

also

$$F(x) = 2\ x^{1/2}\ L(1,\chi) - C\ L\big(\frac{1}{2},\chi\big) + \mathrm{O}(1).$$

Nimmt man $L(1,\chi) = 0$ an, so führt dies zu $F(x) = \mathrm{O}(1)$, was (1.1) widerspricht.

2. Beweis zu den übrigen Fällen.
In Analogie zu dem Ausdruck

$$\mathrm{Re}\Big(3\ \frac{\zeta'}{\zeta}(\sigma) + 4\ \frac{\zeta'}{\zeta}(\sigma+it) + \frac{\zeta'}{\zeta}(\sigma+2it)\Big)$$

beim Beweis zu $\zeta(1+it) \neq 0$ für $t \neq 0$ wird hier

$$A(\sigma,t,\chi) \underset{\text{Df}}{=} \operatorname{Re}\Big(3\,\frac{L'}{L}(\sigma,\chi_0) + 4\,\frac{L'}{L}(\sigma+it,\chi) + \frac{L'}{L}(\sigma+2it,\chi^2)\Big) \tag{2.1}$$

betrachtet. Dabei ist für $\chi^2 \neq \chi_0$ auch $t = 0$ zugelassen, für $\chi^2 = \chi_0, \quad \chi \neq \chi_0$ wird $t \neq 0$ gefordert. Für den Hauptcharakter χ_0 ist wegen 4.5.(2) die Behauptung schon gezeigt. Die Fallunterscheidung erklärt sich daraus, daß für $\chi^2 = \chi_0,\ t = 0$ der Summand $\frac{L'}{L}(\sigma+2it,\chi^2) = \frac{L'}{L}(\sigma,\chi_0)$ einen Pol–Anteil beiträgt und daher der Schluß nicht funktioniert.

Wegen $\sigma > 1$ kann man 4.6.(2) anwenden

$$\begin{aligned} A(\sigma,t,\chi) &= -\operatorname{Re} \sum_{(n,m)=1} \frac{\Lambda(n)}{n^\sigma}\Big(3 + 4\,\chi(n)\,n^{-it} + \big(\chi(n)\,n^{-it}\big)^2\Big) \\ &= -\sum_{(n,m)=1} \Lambda(n)\,n^{-\sigma}\big(3 + 4\cos\varphi_n + \cos(2\varphi_n)\big) \quad \leq 0, \end{aligned} \tag{2.2}$$

wobei $\varphi_n = \arg\big(\chi(n)\,n^{-it}\big)$.
Wie im Beweis zu Satz 2.5. sieht man, da $L(\sigma+2it,\chi^2)$ allenfalls eine Nullstelle einbringt,

$$A(\sigma,t,\chi) = \frac{-3+4\nu+\mu}{\sigma-1} + \text{Beschränktes},$$

wobei $\nu \in \mathbb{N}$ die Ordnung der Nullstelle $1+it$ von $L(s,\chi)$ und $\mu \in \mathbb{N}$ die der Nullstelle $1+2it$ von $L(s,\chi^2)$ bezeichnet. Für $\sigma \to 1^+$ ergibt dies $A(\sigma,t,\chi) \to \infty$, was (2.2) widerspricht. □

Es sind nun alle Hilfsmittel zur Anwendung des Newman'schen Tauber–Satzes bereitgestellt.

4.8. Primzahlsatz in arithmetischen Progressionen (Dirichlet, 1837; Hadamard, de la Vallée–Poussin, 1896).
Sei $m \in \mathbb{N}, \quad (a,m) = 1, \quad x \geq 1$. Dann gilt für $x \to \infty$

$$\begin{aligned} \psi(x,m,a) &\underset{\text{Df}}{=} \sum_{n \leq x n \equiv a(m)} \Lambda(n) = \frac{x}{\varphi(m)}\big(1+\mathrm{o}(1)\big), \\ \pi(x,m,a) &\underset{\text{Df}}{=} \#\{p \leq x,\ p \equiv a(m)\} = \frac{x}{\varphi(m)\ln x}\big(1+\mathrm{o}(1)\big). \end{aligned}$$

Bemerkungen.
1. Wegen des Primzahlsatzes $\pi(x) = \frac{x}{\ln x}\big(1+\mathrm{o}(1),\big)$ (der für $m = a = 1$ hierin enthalten ist) ist die Interpretation „Die Primzahlen sind in den $\varphi(m)$ reduzierten

Restklassen mod m asymptotisch gleichmäßig verteilt“ gerechtfertigt. Zum Beispiel gibt es asymptotisch gleich viele Primzahlen $\equiv 1$ und $\equiv 3 \bmod 4$, , im Sinn

$$\lim_{x\to\infty} \frac{\pi(x,4,1)}{\pi(x,4,3)} = 1.$$

2. Die jeweiligen o–Funktionen können stark von m und a abhängen. Für Aussagen, in denen die Fehlerfunktionen gleichmäßig in m abgeschätzt werden, sind insbesondere explizite untere Schranken für $|L(1,\chi)|$ nötig. Hier sind noch viele Fragen offen.

Zum Beweis.
Da im Prinzip wie bei der Herleitung des gewöhnlichen Primzahlsatzes argumentiert wird, reichen einige Hinweise. Nach 4.6. hat man für $\sigma > 1$

$$\sum_{n\le x n\equiv a(m)} \frac{\Lambda(n)}{n^s} = -\frac{1}{\varphi(m)} \frac{L'}{L}(s,\chi_0) - \frac{1}{\varphi(m)} \sum_{\chi\neq\chi_0} \overline{\chi}(a)\cdot \frac{L'}{L}(s,\chi).$$

Sei $G(s) = \prod_{p|m} \big(1 - \frac{1}{p^s}\big)$. G ist holomorph und $\neq 0$ für $\sigma > 0$. Es gilt somit

$$\frac{L'}{L}(s,\chi_0) = \frac{\zeta'}{\zeta}(s) + \frac{G'}{G}(s), \quad \text{wobei } G'/G \text{ für } \sigma \ge 1 \text{ holomorph ist.}$$

Wegen Satz 4.7. ist für jedes $\chi \neq \chi_0$ $\frac{L'}{L}$ holomorph für $\sigma \ge 1$. Wie beim Beweis zum Primzahlsatz wird der Pol von $-\frac{\zeta'}{\zeta}$ bei 1 durch Subtraktion von $\zeta(s)$ aufgehoben. Man erhält schließlich:

$$\sum_{n\equiv a(m)} \frac{\Lambda(n)}{n^s} - \frac{1}{\varphi(m)}\,\zeta(s)$$

ist holomorph für $\sigma \ge 1$. Ähnlich wie früher sieht man

$$\begin{aligned} F(z) &\underset{\text{Df}}{=} -\sum_{n\equiv a(m)} \frac{\Lambda(n)}{n^{z+1}} - \frac{1}{\varphi(m)}\,\zeta(z+1) \\ &= \int_0^\infty \Big(\frac{\psi(e^t,m,a)}{e^t} - \frac{1}{\varphi(m)}\; frac[e^t]e^t\Big) e^{-tz}\; dt \end{aligned}$$

mit für Re $z \ge 0$ holomorphem F. Der Newman'sche Tauber–Satz ist anwendbar und liefert

$$\frac{\psi(e^t,m,a)}{e^t} \to \frac{1}{\varphi(m)} \quad \text{für} \quad t\to\infty,$$

was der Behauptung für ψ entspricht. Der Übergang von $\psi(x,m,a)$ zu $\pi(x,m,a)$ erfolgt wie früher. □

5. Kapitel. Siebmethoden

Die Grundfragen dieses Gebietes kann man am ältesten und einfachsten Verfahren, dem Sieb des Eratosthenes, gut studieren.

Es sollen die Primzahlen p unterhalb einer großen Zahl x aufgelistet, oder zumindest deren Anzahl bestimmt werden. Die Primzahlen bis $\sqrt{x}$ seien schon bekannt. Dann besteht das Sieb darin, dass man für jedes $p \leq \sqrt{x}$ die durch p teilbaren Zahlen $\leq x$ streicht. Oder: Man entfernt für die $p \leq \sqrt{x}$ jeweils die Null–Restklasse. Übrig bleiben die Zahl 1 und die Primzahlen $\in (\sqrt{x}, x]$. Ein allgemeines „Sieb“ kann so aussehen.

Gegeben

a) Eine Menge M ganzer Zahlen (bei Eratosthenes die $n \in [1, x]$),

b) eine Menge $\mathcal{P}$ von Primzahlen p (bei Eratosthenes die $p \in (1, \sqrt{x}]$),

c) zu jedem $p \in \mathcal{P}$ eine Menge $\Omega(p)$ von Restklassen (bei Eratosthenes jeweils die Null–Restklasse). Zu jedem $p \in \mathcal{P}$ streiche man aus M alle n, die in einer der $\omega(p)$ Restklassen aus $\Omega(p)$ $(\omega(p) = \#\,\Omega(p))$ liegen. Gesucht sind Aussagen über die Menge der nicht gestrichenen Zahlen, z.B. untere und obere Abschätzungen für die Anzahl.

Ein wichtiges Beispiel: x groß, $M = \mathbb{N} \cap [1, x]$, $\mathcal{P} = \{p \leq \sqrt{x}\}$

$$\Omega(2) = \{0 + 2\mathbb{Z}\}, \quad \Omega(p) = \{0 + p\mathbb{Z}, -2 + p\mathbb{Z}\} \quad \text{für} \quad 2 < p \leq \sqrt{x}.$$

Für $2 < p \leq \sqrt{x}$ streicht man die Zahlen n, für die $n \equiv 0(p)$ oder $n + 2 \equiv 0(p)$ ist. Es bleiben also die ungeraden Zahlen $n \leq x$, für die weder n noch $n + 2$ durch eine Primzahl $\leq \sqrt{x}$ teilbar ist. Dies sind genau die Primzahlen p mit $\sqrt{x} < p \leq x - 2$, für die auch $p + 2$ prim ist, im wesentlichen also die „Primzahlzwillinge“ (genauer: das jeweils kleinere der Geschwister) zwischen $\sqrt{x}$ und x.

Ein solches algemeines „**Sieb**“ wird also durch ein Tripel

$$(M, \mathcal{P}, \Omega) \quad \Omega(p) \subset \mathbb{Z}/p\,\mathbb{Z}, \quad 0 \leq \omega(p) = \#\,\Omega(p) < p \tag{S1}$$

beschrieben. Die Forderung $\omega(p) < p$ ist keine Einschränkung. Denn $\omega(p) = p$ würde heißen, dass alle Restklassen mod p ausgesondert werden, d.h. dass keine Zahlen übrig bleiben.

Ein Sieb kann auch anders beschrieben werden. Man hat eine Folge von N ganzen Zahlen $a_1, \ldots, a_N$ und wie oben eine Menge $\mathcal{P}$ von Primzahlen p. Gefragt ist nach der Anzahl S

der Zahlen $1 \le n \le N$, für die a_n zu allen $p \in \mathcal{P}$ teilerfremd ist. Oder, wenn $P = \prod_{p \in \mathcal{P}} p$ gesetzt wird,

(S2) $$S = \#\{1 \le n \le N, \quad (a_n, P) = 1\}.$$

Mit diesem Konzept kann auch das Zwillingsproblem formuliert werden. $N = [x]$, $a_n = n(n+2)$, $\mathcal{P} = \{p \le \sqrt{x}\}$. Dann zählt S genau die Primzahlzwillinge $(p, p+2)$ mit $\sqrt{x} < p \le x - 2$.

Man kann sich überlegen, dass beide Zugänge in den meisten konkreten Problemen auf das gleiche hinauslaufen.

Das Eratosthenes–Sieb im Sinn des zweiten Konzepts kann – mit $a_n = n$ für $1 \le n \le x$ und $P = \prod_{p \le \sqrt{x}} p$ – so formuliert werden.

(E1) $$\pi(x) - \pi(\sqrt{x}) + 1 = \#\{n \le x, \quad (n, P) = 1\}.$$

Nach Legendre wird die rechte Seite umgeformt zu

(E2) $$\sum_{d|P} \mu(d) \sum_{\substack{n \le x \\ n \equiv 0 (d)}} 1 = x \sum_{d|P} \frac{\mu(d)}{d} + \sum_{d|P} \mu(d) \Big(\Big[\frac{x}{d} \Big] - \frac{x}{d} \Big).$$

Wegen der gewaltigen Zahl der Teiler von P – es sind $2^{\pi(\sqrt{x})}$ Stück – ist es nicht möglich, den zweiten Term vernünftig auszuwerten. Dementsprechend ist es bis heute nicht gelungen, auf diesem Weg den Primzahlsatz zu beweisen.

Es ist klar, dass die Menge der nicht gestrichenen Zahlen größer wird, wenn man die Menge der Sieb–Primzahlen verkleinert. Zum Beispiel beim Zwillingsproblem erweist es sich als nützlich, statt der Grenze $\sqrt{x}$ für die Sieb–Primzahlen eine kleine x–Potenz $z = x^c$ zu nehmen. Dies ist der Hauptgrund dafür, dass man mit Siebmethoden eher obere Schranken als untere erhält. Dies wird sich auch hier beim Zwillingsproblem bestätigen.

In den letzten ca. 90 Jahren sind im wesentlichen drei Methoden entwickelt worden, die bei den klassischen Problemen wie dem Goldbachschen oder dem Zwillingsproblem zu etwa den gleichen Ergebnissen führen.

1. Das Brunsche Sieb, ab 1920 (Viggo B., 1885–1978).
Die einfache Grund–Idee ist, in (E2) und entsprechend in der allgemeineren Situation (S2)

„kleine“ Teilmengen $\mathcal{D}^-$ und $\mathcal{D}^+$ von $\mathcal{D} = \{d|P\}$ zu finden mit

$$\sum_{d\in\mathcal{D}^-} \mu(d)\,\#\{n\le N,\ \ d|a_n\} \le\ \#\{n\le N,\ \ (a_n,P)=1\} \le \sum_{d\in\mathcal{D}^+} \mu(d)\ \#\ \{n\le N,\ \ d|a_n\}.$$

Dies ist ein ernstes kombinatorisches Problem. Die Durchführung ist sehr verwickelt.

2. Das Selbergsche Sieb, 1947 (Atle S., geb. 1917).
Auch hier ist die Grund–Idee einfach und wirkt etwas verwegen. Es seien vorläufig die Zahlen $\lambda(1),\dots,\lambda(z)$ $(z\in\mathbb{N}$ ein später zu wählender Parameter) beliebig reell, außer der Festlegung $\lambda(1)=1$. Dann gilt

$$\#\big\{n\le N,\ \ (a_n,P)=1\big\} \le \sum_{n\le N}\Big(\sum_{d|P,\,d\le z,\,d|a_n}\lambda(d)\Big)^2.$$

Denn im Fall $(a_n,P)=1$ ist die innere Summe $=1$, ansonsten ist sie ≥ 0. Durch raffinierte elementare Umformungen ist es vielfach möglich, die für das Problem optimalen λ zu finden und so tatsächlich eine den Erwartungen entsprechende obere Abschätzung zu erzielen.

3. Das große Sieb.
Mit Linnik begann 1941 ein Zweig der Zahlentheorie, der nicht nur bei Sieb–Fragen anwendbar ist. 1968 konnte Hugh L. Montgomery zeigen, dass man hiermit relativ rasch zu einer oberen Sieb–Abschätzung kommt, die in vielen Fällen die Brunschen und Selbergschen Ergebnisse einschließt. Dieser Zugang soll hier dargestellt werden. Dass dabei eine Siebmethode entsteht, wird erst relativ spät sichtbar.

5.1. Satz (Große–Sieb–Ungleichung)
Für $x,\ Q\ge 1,\ \alpha_n\in\mathbb{C}\ (1\le n\le x)$ sei

$$S(t)=\sum_{n\le x}\alpha_n\,e(nt)\quad\big(t\in\mathbb{R},\ \ e(\beta)=e^{2\pi i\beta}\big).$$

Dann gilt

$$\sum_{k\le Q}\sum_{\substack{1\le a\le k\\(a,k)=1}}\Big|S\Big(\frac{a}{k}\Big)\Big|^2 \le (Q^2+2\pi x)\ \sum_{n\le x}|\alpha_n|^2.$$

Beweis.
1. Im weiteren, auch im Beweis zum nächsten Satz, soll $\sum\limits^{*}_{a \bmod k}$ Summation über ein reduziertes Restsystem mod k bedeuten. Dies hat nur Sinn, wenn die Summanden k–periodisch sind. Bei $|S(\ )|$ ist dies der Fall

$$S\Big(\frac{a+gk}{k}\Big)=\sum_n\alpha_n\,e\Big(\frac{a}{k}\,n+gn\Big)=S\Big(\frac{a}{k}\Big),$$

denn $e(\cdot)$ ist 1–periodisch. Die hier benutzten k seien stets $\leq Q$, und es gelte $(a,k)) = 1$.

2. Sei $\delta = \frac{1}{2}\, Q^{-2}$. Dann sind die Intervalle

$$I_{k,a} = \Big[\frac{a}{k} - \delta, \frac{a}{k} + \delta\Big]$$

bis auf einen eventuellen gemeinsamen Endpunkt paarweise disjunkt. Denn für $\dfrac{a}{k} \neq \dfrac{a'}{k'}$ ist

$$\Big|\frac{a}{k} - \frac{a'}{k'}\Big| = \Big|\frac{ak' - a'k}{kk'}\Big| \geq Q^{-2}|ak' - a'k| \geq Q^{-2},$$

da $ak' - a'k \in \mathbb{Z}\backslash\{0\}$.

3. Die Funktion $F(t) = S^2(t)$ ist 1–periodisch und stetig differenzierbar. Es ist $\displaystyle\int_{\frac{a}{k}}^{t} F'(s)\, ds = F(t) - F\big(\frac{a}{k}\big)$, also

$$\Big|F\Big(\frac{a}{k}\Big)\Big| \leq \big|F(t)\big| + \Big|\int\limits_{\frac{a}{k}}^{t} \big|F'(s)\big|\, ds\Big|,$$

integriert über $I_{k,a}$ somit

$$2\delta\Big|F\Big(\frac{a}{k}\Big)\Big| \leq \int\limits_{I_{k,a}} \big|F(t)\big|\, dt + \delta \int\limits_{I_{k,a}} \big|F'(t)\big|\, dt. \tag{3}$$

4. Wegen 2. füllen die $I_{k,a}$ das verschobene Einheitsintervall $[\delta, 1+\delta]$ höchstens einmal aus. Summation von (3) über k und a sowie die Periodizität von F und $F' = 2S\ S'$ ergeben

$$2\delta \sum_{k,a} \Big|S^2\Big(\frac{a}{k}\Big)\Big| \leq \int\limits_0^1 \big|S^2(t)\big|\, dt + 2\delta \int\limits_0^1 \big|S'(t)\big|\ \big|S(t)\big|\, dt,$$

also nach Anwendung der Cauchy–Schwarzschen Ungleichung

$$\sum_{k,a} \Big|S^2\Big(\frac{a}{k}\Big)\Big| \leq Q^2 \int\limits_0^1 \big|S^2(t)\big|\, dt + \Big(\int\limits_0^1 \big|S^2(t)\big|\, dt\Big)^{1/2}\ \Big(\int\limits_0^1 \big|S'^2(t)\big|\, dt\Big)^{1/2}. \tag{4}$$

5. Mit der Orthogonalitätsrelation sieht man

$$\begin{aligned}\int\limits_0^1 \big|S^2(t)\big|\, dt &= \sum_{n_1 \leq x}\ \sum_{n_2 \leq x} \alpha_{n_1}\overline{\alpha}_{n_2} \int\limits_0^1 e^{2\pi i(n_1 - n_2)t}\, dt \\ &= \sum_{n \leq x} |\alpha_n|^2\end{aligned}$$

und analog

$$\int_0^1 \left|S'^2(t)\right| dt = \sum_{n_1 \le x} \left(2\pi i\, n_1\ \alpha_{n_1}\right)\ \sum_{n_2 \le x} \left(-2\pi i\, n_2\ \overline{\alpha}_{n_2}\right)\ \int_0^1 e^{2\pi i (n_1 - n_2) t}\, dt$$
$$\le (2\pi x)^2 \sum_{n \le x} |\alpha_n|^2.$$

Einsetzen in (4) liefert die Behauptung. □

5.2. Satz von Montgomery, 1968.
$x, Q \ge 1$. Für jedes $p \le Q$ sei $\Omega(p)$ eine Menge von $\omega(p)$ Restklassen mod p. Es gelte $0 \le \omega(p) < p$. $\mathcal{A}$ sei die Teilmenge von $\mathbb{N} \cap [1, x]$, die entsteht, wenn für jedes $p \le Q$ die Restklassen $\in \Omega(p)$ gestrichen werden. Dann gilt

$$A = \#\ \mathcal{A} \le \left(Q^2 + 2\pi x\right) L^{-1}$$

mit

$$L = \sum_{k \le Q} \mu^2(k)\ \prod_{p \mid k}\ \frac{\omega(p)}{p - \omega(p)}\,.$$

Bemerkungen.
1. $\mathcal{A}$ entsteht offenbar durch einen Sieb–Prozess. Statt der Ausgangszahlen $\mathbb{N} \cap [1, x]$ können auch die Zahlen in irgendeinem Intervall der Länge x genommen werden.

2. Mit wachsendem $\omega(p)$ wächst auch L, denn für $\omega(p) \le p - 2$ ist

$$\frac{\omega(p)}{p - \omega(p)}\ \le\ \frac{\omega(p) + 1}{p - (\omega(p) + 1)}\,.$$

Dies entspricht der Erwartung, dass die Menge der nicht gestrichenen Zahlen höchstens abnimmt, wenn man mehr Restklassen entfernt.

3. Es kommt darauf an, eine gute untere Schranke für L zu finden. Dies kann mühsam sein.

4. Während Brunsches und Selbergsches Sieb am besten zu handhaben sind, wenn $\omega(p)$ beschränkt ist („kleine Siebe“), kann hier $\omega(p)$ mit p wachsen („großes Sieb“). Der Nachteil des Montgomery–Siebes ist, dass die zu siebenden Zahlen die $n \in [1, x]$ sind, während die anderen Siebe auch schnell wachsende Folgen, wie etwa die Werte eines Polynoms, wirksam erfassen können. Bei den vorgesehenen Anwendungen spielt dies keine Rolle.

Beweis zu Satz 5.2.

1. Es wird ausreichen, die folgende Aussage zu beweisen. Sei $\alpha_n \in \mathbb{C}$ für $1 \le n \le x$ und $\alpha_n = 0$ für $n \notin \mathcal{A}$, $g(p) = \dfrac{\omega(p)}{p - \omega(p)}$ und für $\mu^2(k) = 1$ $g(k) = \prod\limits_{p|k} g(p)$. Dann gilt für $\mu^2(k) = 1$

$$(1) \qquad g(k) \Big|\sum_n \alpha_n\Big|^2 \le \sum_{a \bmod k}^{*} \Big|S\Big(\frac{a}{k}\Big)\Big|^2 \quad \big(S(t) = \sum_n \alpha_n\, e(nt)\big).$$

Zum Beweis des Satzes nehme man einfach

$$\alpha_n = 1, \quad \text{falls} \quad n \in \mathcal{A}, \quad = 0 \quad \text{sonst.}$$

Dann ist $\sum\limits_n \alpha_n = \sum\limits_n \alpha_n^2 = A$. Summation von (1) über $k \le Q$ ergibt

$$\sum_{k \le Q} \mu^2(k)\, g(k) \cdot A^2 \le \sum_{k \le Q} \sum_{a \bmod k}^{*} \Big|S\Big(\frac{a}{k}\Big)\Big|^2.$$

Die rechte Seite ist nach Satz 5.1. $\le (Q^2 + 2\pi x)\, A$. Dies entspricht der Behauptung des Satzes.

2. (1) wird durch Induktion nach der Anzahl der Primfaktoren von k bewiesen. Zuerst also die Aussage für $k = p \le Q$, d.h.

$$(1\text{p}) \qquad \frac{\omega(p)}{p - \omega(p)} \Big|\sum_n \alpha_n\Big|^2 \le \sum_{a=1}^{p-1} \Big|S\Big(\frac{a}{p}\Big)\Big|^2.$$

Sei $Z = \sum\limits_n \alpha_n$, $Z(p,h) = \sum\limits_{n \equiv h(p)} \alpha_n$. Dann ist

$$\begin{aligned}\sum_{a=1}^{p-1} \Big|S\Big(\frac{a}{p}\Big)\Big|^2 &= \sum_{n_1} \sum_{n_2} \alpha_{n_1}\, \overline{\alpha}_{n_2} \sum_{a=1}^{p-1} e\Big(n_1\, \frac{a}{p}\Big)\, e\Big(-n_2\, \frac{a}{p}\Big) \\ &= \sum_{n_1, n_2} \alpha_{n_1}\, \overline{\alpha}_{n_2} \Big(\sum_{a=0}^{p-1} e\Big(\frac{a}{p}\,(n_1 - n_2)\Big) - 1\Big).\end{aligned}$$

Die innere Summe ist eine geometrische Reihe mit dem Wert 0, falls $n_1 \not\equiv n_2 \bmod p$ und $= p$, falls $n_1 \equiv n_2 \bmod p$.

$$\begin{aligned}\sum_{a=1}^{p-1} \Big|S\Big(\frac{a}{p}\Big)\Big|^2 &= p \sum_{\substack{n_1, n_2 \\ n_1 \equiv n_2 \bmod p}} \alpha_{n_1}\, \overline{\alpha}_{n_2} - |Z|^2 \\ &= p \sum_{h=0}^{p-1} \big|Z(p,h)\big|^2 - |Z|^2\end{aligned}$$

oder

$$\sum_{h=0}^{p-1} \big|Z(p,h)\big|^2 = \frac{1}{p}\Big(\sum_{a=1}^{p-1} \Big|S\Big(\frac{a}{p}\Big)\Big|^2 + |Z|^2\Big). \tag{2}$$

Die Anzahl der $h \in \{0,\dots,p-1\}$ mit $Z(p,h) \neq 0$ ist $\leq p - \omega(p)$. Mit der Cauchy–Schwarz–Ungleichung und (2) folgt

$$\begin{aligned}
\big|Z\big|^2 = \Big|\sum_{h=0}^{p-1} Z(p,h)\Big|^2 &\leq \Big(\sum_{\substack{h=0\\ Z(p,h)\neq 0}}^{p-1} 1\Big)\ \Big(\sum_{h=0}^{p-1} \big|Z(p,h)\big|^2\Big) \\
&\leq \big(p-\omega(p)\big)\ \frac{1}{p}\ \Big(\big|Z\big|^2 + \sum_{a=1}^{p-1}\ \Big|S\Big(\frac{a}{p}\Big)\Big|^2\Big) \\
&= \frac{p-\omega(p)}{p}\ \big|Z\big|^2 + \frac{p-\omega(p)}{p}\ \sum_{a=1}^{p-1}\ \Big|S\Big(\frac{a}{p}\Big)\Big|^2
\end{aligned}$$

und damit

$$\big|Z\big|^2\ \Big(1 - \frac{p-\omega(p)}{p}\Big) \leq \frac{p-\omega(p)}{p}\ \sum_{a=1}^{p-1}\ \Big|S\Big(\frac{a}{p}\Big)\Big|^2,$$

woraus sich unmittelbar (1p) ergibt.

3. Es sei nun $\mu^2(k) = 1$, $k = k_1k_2$, wobei k_1 und k_2 mindestens einen Primfaktor haben. Es werde vorausgesetzt, dass (1) für k_1, k_2 und alle in Frage kommenden Koeffizienten α_n schon gezeigt ist.

Nach Wahl von k, k_1 und k_2 ist $(k_1,k_2) = 1$. Durchläuft a ein reduziertes Restsystem mod k_1 und b eins mod k_2, dann durchläuft $ak_2 + bk_1$ eins mod $k_1k_2 = k$.
Mit der 1–Periodizität von $S(t)$ ergibt sich

$$\sum_{c \bmod k}^{*}\ \Big|S\Big(\frac{c}{k}\Big)\Big|^2 = \sum_{a(k_1)}^{*}\ \sum_{b(k_2)}^{*}\ \Big|S\Big(\frac{a}{k_1} + \frac{b}{k_2}\Big)\Big|^2. \tag{3}$$

Bei festgehaltenem a hat $S\Big(\frac{a}{k_1} + \frac{b}{k_2}\Big)$ die Gestalt $\sum\limits_n \alpha_n\ e\Big(\frac{a}{k_1}\,n\Big)\ e\Big(\frac{b}{k_2}\,n\Big)$.
Setzt man $\beta_n = \beta_{n,a} = \alpha_n\ e\Big(\frac{a}{k_1}\,n\Big)$, dann ist auf die Summe $T(t) = \sum\limits_n \beta_n\ e(t)$ die

Induktionsvoraussetzung bezüglich k_2 anwendbar.

$$\begin{aligned}\sum_{b(k_2)}^{*} \Big|S\Big(\frac{a}{k_1}+\frac{b}{k_2}\Big)\Big|^2 &= \sum_{b(k_2)}^{*} \Big|T\Big(\frac{b}{k_2}\Big)\Big|^2 \\ \geq g(k_2)\,\Big|\sum_n \beta_n\Big|^2 &= g(k_2)\,\Big|\sum_n \alpha_n\, e\Big(\frac{a}{k_1}\,n\Big)\Big|^2 \\ &= g(k_2)\,\Big|S\Big(\frac{a}{k_1}\Big)\Big|^2.\end{aligned}$$

Mit der Induktionsvoraussetzung für k_1, angewandt auf die α_n, folgt daraus

$$\begin{aligned}\sum_{c \bmod k}^{*} \Big|S\Big(\frac{a}{k}\Big)\Big|^2 &\geq g(k_2)\,g(k_1)\,\Big|\sum_n \alpha_n\Big|^2 \\ &= g(k)\,\Big|\sum_n \alpha_n\Big|^2,\end{aligned}$$

was zu zeigen war.

Für $k=1$ ist wegen $S\Big(\frac{1}{1}\Big)=\sum_n \alpha_n$ nichts zu beweisen. □

Im Briefwechsel zwischen **Euler** und **Goldbach** (Christian von G., 1690–1764) kam 1742 die Frage auf, ob

a) jede gerade Zahl ≥ 4 Summe zweier Primzahlen (**binäres Problem**) und

b) jede ungerade Zahl ≥ 7 Summe dreier Primzahlen (**ternäres Problem**) ist.

Mit Brunschen Sieb–Abschätzungen und den Additionssätzen für Zahlenmengen konnte Schnirelman 1933 ein erstes in diese Richtung gehendes Resultat zeigen: Es gibt ein c, so dass jedes $n \geq 2$ als Summe von höchstens c Primzahlen geschrieben werden kann. Dies soll hier ausgeführt werden.

Das ternäre Problem – für hinreichend großes ungerades $n \in \mathbb{N}$ – wurde 1937 von I.M. Vinogradov mittels der Hardy–Littlewoodschen Kreismethode gelöst. Das binäre wartet bis heute auf eine Antwort.

Im Folgenden sollen $c_1, c_2, \ldots$ positive, universelle, im Prinzip numerisch angebbare Konstanten sein.

5.3. Satz. Sei $N \in \mathbb{N}$, $N \equiv 0 \bmod 2$, $N \geq 4$. Dann besteht die Ungleichung

$$\#\big\{p \leq N,\ N-p \text{ prim}\big\} = \#\big\{(p_1,p_2),\ N=p_1+p_2\big\} \leq c_1\,\frac{N}{(\ln N)^2}\,\prod_{p\mid N}\Big(1-\frac{1}{p}\Big)^{-1}.$$

Bemerkung. N hat $N-1$ Zerlegungen $N = n_1 + n_2$. Auf Grund der Häufigkeit der Primzahlen wird man vermuten, dass es ungefähr $\dfrac{N}{(\ln N)^2}$ Darstellungen $N = p_1 + p_2$ gibt. Dies wird durch die Ungleichung, zumindest nach oben, bestätigt. Der Produktfaktor kann bei vielen Primfaktoren von N beliebig groß werden.

Beweis zu 5.3.
1. Die abzuschätzende Anzahl werde mit $G(N)$ abgekürzt. N sei vorläufig als groß vorausgesetzt. Mit später geeignet festzulegendem $z = N^{c_2} \in (5, N^{1/2}]$ wird im Hinblick auf Satz 5.2

$$
\begin{aligned}
&\omega(p) = 1, \quad \Omega(p) = \{0 + p\,\mathbb{Z}\} \text{ für } \ p|N, \ \ p \le z, \\
&\omega(p) = 2, \quad \Omega(p) = \{0 + p\,\mathbb{Z},\ N - p + p\,\mathbb{Z}\} \text{ für } \ p \not| N,\ p \le z \\
&\omega(p) = 0 \quad \text{für} \quad p > z
\end{aligned} \tag{1.1}
$$

gesetzt. $\mathcal{A} \subset [1, N] \cap \mathbb{N}$ entstehe durch Streichen der Restklassen aus $\Omega(p)$ für alle $p \le z$. Primzahlen $q \in (z, N - z]$, für die $N - q$ prim ist, werden nicht gestrichen, denn andernfalls wäre $q \equiv \mathrm{o}(p)$ für ein $p \le z$ oder $q \equiv N - p(p)$ bzw. $N - q \equiv \mathrm{o}(p)$ für ein $p \le z$. Jedes $q \in (z, N - z]$, das in $G(N)$ gezählt wird, liegt also in $\mathcal{A}$. Man erhält daher mit $A = \#\,\mathcal{A}$

$$G(N) \le A + 2z. \tag{1.2}$$

2. Satz 5.2. mit $x = N$ und $Q = N^{1/2}$ ergibt

$$A \le (2\pi + 1)\, N\, L^{-1}, \tag{2.1}$$

wobei

$$L = \sum_{k \le Q,\, p|k \Rightarrow p \le z} \mu^2(k) \prod_{p|k} \frac{\omega(p)}{p - \omega(p)}. \tag{2.2}$$

3. Es wird darauf ankommen, L mit der vollen Summe

$$S = \sum_{k,\, p|k \,\Rightarrow\, p \le z} \mu^2(k)\, g(k), \ \ g(p) = \frac{\omega(p)}{p - \omega(p)} \tag{3.1}$$

zu vergleichen. Setzt man $P = \prod\limits_{p \le z} p$, dann kann S als $\sum\limits_{d|P} g(d)$ geschrieben werden und somit

$$S = \prod_{p \le z} \big(1 + g(p)\big) = \exp\Big(\sum_{p \le z} \ln\big(1 + g(p)\big)\Big).$$

Für alle p ist

$$0 \le g(p) \le \frac{2}{p/3} = \frac{6}{p}. \tag{3.2}$$

Durch Entwickeln erhält man $\ln\big(1+g(p)\big) = g(p) + \mathrm{O}(p^{-2})$,

$$\begin{aligned}\sum_{p\le z} \ln\big(1+g(p)\big) &= \sum_{\substack{p\le z\\ p\mid N}} \frac{1}{p-1} + \sum_{\substack{p\le z\\ p\nmid N}} \frac{2}{p-2} + \mathrm{O}\Big(\sum_{p\le z} \frac{1}{p^2}\Big)\\ &= \sum_{\substack{p\le z\\ p\mid N}} \frac{1}{p} + \sum_{\substack{p\le z\\ p\nmid N}} \frac{2}{p} + \mathrm{O}\Big(\sum_{p\le z} \frac{1}{p^2}\Big)\\ &= 2\sum_{p\le z} \frac{1}{p} - \sum_{\substack{p\le z\\ p\mid N}} \frac{1}{p} + \mathrm{O}(1).\end{aligned}$$

Es wird die in der elementaren Zahlentheorie bewiesene Formel $\displaystyle\sum_{p\le z} \frac{1}{p} = \ln\ln z + \mathrm{O}(1)$ benutzt, sowie $\displaystyle\sum_{p\mid N, p>z} \frac{1}{p} \le \frac{c_3}{z} \le c_4$. Dies ergibt

$$\begin{aligned}S &= \exp\Big(2\ln\ln z - \sum_{p\mid N} \frac{1}{p} + \mathrm{O}(1)\Big)\\ &= \exp\Big(2\ln\ln z + \sum_{p\mid N} \ln\Big(1-\frac{1}{p}\Big) + \mathrm{O}(1)\Big),\end{aligned}$$

$$S \ge c_5 (\ln z)^2 \prod_{p\mid N} \Big(1-\frac{1}{p}\Big). \tag{3.3}$$

4. Dass für genügend kleines z die Summe L, die nur bis Q erstreckt ist, beispielsweise die Hälfte der vollen Summe S erreicht, sieht man mit einer Idee von **Rankin** (1938, Robert A. R., 1915–2001). Sei

$$0 < \eta < \frac{1}{4} \tag{4.1}$$

(später geeignet festzulegen).
Dann ist

$$\begin{aligned}R \underset{\text{Df}}{=} S - L &= \sum_{k>Q} \mu^2(k)\, g(k)\\ &\le \sum_{k>Q} \mu^2(k)\, g(k)\, \Big(\frac{k}{Q}\Big)^{\eta} \le \sum_{k} \mu^2(k)\, g(k) \Big(\frac{k}{Q}\Big)^{\eta}\\ &= Q^{-\eta} \prod_{p\le z} \big(1 + g(p)\, p^{\eta}\big).\end{aligned} \tag{4.2}$$

Mit Überlegungen ähnlich wie in 3. sieht man

$$\begin{aligned}\prod_{p\le z}\big(1+g(p)\,p^{\eta}\big) &\le \exp\Big(\sum_{p\le z} g(p)\,p^{\eta}+\mathrm{O}(1)\Big)\\ &= \exp\Big(\sum_{p\le z} g(p)+\sum_{p\le z} g(p)\,\big(p^{\eta}-1\big)+\mathrm{O}(1)\Big)\\ &= (\ln z)^2\prod_{p\mid N}\Big(1-\frac{1}{p}\Big)\exp\Big(\sum_{p\le z} g(p)\,(p^{\eta}-1)+\mathrm{O}(1)\Big). \qquad (4.3)\end{aligned}$$

Mit (3.2) folgt

$$\begin{aligned}\sum_{p\le z} g(p)\,(p^{\eta}-1) &\le 6\sum_{p\le z}\frac{p^{\eta}-1}{p} = 6\sum_{p\le z}\frac{1}{p}\sum_{\nu\ge 1}\frac{(\eta\ln p)^{\nu}}{\nu!}\\ &\le 6\sum_{\nu\ge 1}\frac{(\ln z)^{\nu-1}\eta^{\nu}}{\nu!}\sum_{p\le z}\frac{\ln p}{p}.\end{aligned}$$

In der elementaren Zahlentheorie wurde $\displaystyle\sum_{p\le z}\frac{\ln p}{p}\le c_6\ln z$ gezeigt, also

$$\sum_{p\le z} g(p)\,(p^{\eta}-1)\le c_7\sum_{\nu\ge 1}\frac{(\eta\ln z)^{\nu}}{\nu!} < c_7\,z^{\eta}.$$

Daraus wird mit (3.2)

$$R\le (\ln z)^2\prod_{p\mid N}\Big(1-\frac{1}{p}\Big)\exp\big(-\eta\ln Q+c_8\,z^{\eta}\big).$$

Es fragt sich nun, ob es möglich ist, $\eta\in(0,1/4)$ und $z=N^{c_2}$ so zu wählen, dass

$$F=\exp(-\eta\ln Q+c_7\,z^{\eta})\le\frac{1}{2}\,c_5 \qquad (4.4)$$

gesichert ist. Setzt man

$$\eta=(\ln z)^{-1}\ln\Big(\frac{\ln Q}{\ln z}\Big)=\frac{1}{c_2\ln N}\ln\Big(\frac{1}{2c_2}\Big),$$

dann ist

$$-\eta\ln Q+c_8\,z^{\eta}=-\frac{1}{2c_2}\ln\Big(\frac{1}{2c_2}\Big)+c_8\,\frac{1}{2c_2}.$$

Dabei liegt c_8 fest, c_2 ist beliebig klein wählbar. Für genügend kleines c_2 wird der letzte Ausdruck $\le -\dfrac{1}{4c_2}\ln\Big(\dfrac{1}{2c_2}\Big)$, und es lässt sich (4.4) erfüllen. Für hinreichend großes N,

hat man einmal c_2 festgehalten, ist auch $0 < \eta < 1/4$ richtig.
Hieraus und mit (3.3) ergibt sich schließlich

$$L \geq c_9 (\ln N)^2 \prod_{p|N} \Big(1 - \frac{1}{p}\Big)$$

für $N \geq c_{10}$. Dies entspricht nach (2.1) und (2.2) der Behauptung des Satzes für die $N \geq c_{10}$. Für die endlich vielen $N < c_{10}$ ist die behauptete Ungleichung mit einer evtl. größeren Konstanten ohne weiteres erfüllt. Damit ist Satz 5.3. bewiesen. □

In ähnlicher Weise erhält man die Brunsche Abschätzung für die Primzahl–Zwillinge

5.4. Satz (Viggo Brun, 1920). Für $x \geq 2$ gilt

$$\#\{p \leq x,\ p+2 \text{ prim }\} \leq c_{11} \frac{x}{(\ln x)^2}.$$

Man vermutet, dass diese Ungleichung für $x \geq 3$ mit einem positiven c_{12} auch mit $\geq$ erfüllt ist. Ein Beweis dafür ist nicht in Sicht.

Dass es wesentlich weniger Zwillinge als Primzahlen gibt, illustriert der folgende Satz von Brun.

5.5. Satz. Es gibt ein c_{13}, so dass

$$\sum_{p,p+2 \text{ prim}} \frac{1}{p} \leq c_{13}.$$

Beweis. Für $k \geq 1$ lässt sich der Abschnitt $\displaystyle\sum_{\substack{2^k < p \leq 2^{k+1} \\ p+2 \text{ prim}}} \frac{1}{p}$ nach 5.4. abschätzen durch

$$\leq \frac{1}{2^k}\ c_{11}\ \frac{2^{k+1}}{(\ln 2^{k+1})^2} = \frac{2c_{11}}{(\ln 2)^2 (k+1)^2}.$$

Die Summe über alle k konvergiert. □

Die obere Schranke für die Anzahl der „Goldbach–Darstellungen“ in Satz 5.3. wird ähnlich wie beim Beweis von Schnirelman–Linnik für die abgeschwächte Lösung des Goldbach–Problems benutzt.

5.7. Satz (Brun–Schnirelman). Es gibt eine Konstante K, so dass jedes $n \geq 2$ als Summe von höchstens K Primzahlen darstellbar ist.

Bem. Während der Schnirelmansche Wert für K bei 800 000 lag, ist man inzwischen durch zahlreiche methodische Neuerungen bei $K = 7$ angekommen. (Ramaré, 1997).

Beweis.
1. Sei

$$\mathcal{A} = \{n \in \mathbb{N},\ \exists p_1, p_2 :\ n = p_1 + p_2\} \cup \{0, 1\}, \tag{1.1}$$
$$G(n) = \#\big\{(p_1, p_2),\ p_1 + p_2 = n\big\}.$$

Die Cauchy–Schwarzsche Ungleichung ergibt

$$\Big(\sum_{n\le x} G(n)\Big)^2 \le \#\big\{n \le x,\ \ G(n) > 0\big\} \cdot \sum_{n\le x} G^2(n).$$

Für $x \ge 4$ erhält man mit Tschebytschev

$$\begin{aligned}\sum_{n\le x} G(n) &\ge \sum_{n\le x} \big\{p_1, p_2 \le \frac{x}{2},\ \ p_1 + p_2 = n\big\} \\ &= \Big(\pi\Big(\frac{x}{2}\Big)\Big)^2 \ge c_1\ \frac{x^2}{(\ln x)^2},\end{aligned}$$

$$\#\big\{n \le x,\ G(n) > 0\big\} \ge c_2\ \frac{x^4}{(\ln x)^4}\ \Big(\sum_{n\le x} G^2(n)\Big)^{-1}. \tag{1.2}$$

2. Für ungerade n ist $G(n) \le 2$, für gerade n wird Satz 5.3. angewandt.

$$\begin{aligned}\sum_{n\le x} G^2(n) &\le 2x + c_3 \sum_{2\le n\le x} \frac{n^2}{(\ln n)^4} \prod_{p|n} \Big(1 - \frac{1}{p}\Big)^{-2} \\ &\le 2x + c_4\ \frac{x^2}{(\ln x)^4} \sum_{n\le x} \prod_{p|n} \Big(1 + \frac{2}{p}\Big). \qquad (2.1)\end{aligned}$$

Mit $d(k) = \mathrm{O}(k^{1/2})$ erhält man

$$\begin{aligned}\sum_{n\le x} \prod_{p|n} \Big(1 + \frac{2}{p}\Big) &\le \sum_{n\le x} \sum_{k|n} \mu^2(k)\ \frac{2^{\omega(k)}}{k} \\ &\le \sum_{n\le x} \sum_{k|n} \frac{d(k)}{k} \le \sum_{k\le x} \frac{d(k)}{k} \cdot \frac{x}{k} \le c_5 x\end{aligned}$$

und somit

$$\sum_{n\le x} G^2(n) \le c_6\ \frac{x^3}{(\ln x)^4}.$$

3. Zusammenfassung von 2. und 1. führt zu

$$\#\{n \le x,\ G(n) > 0\} \ge c_7 x \quad \text{für} \quad x \ge 4,$$

oder, nach (1.1),

$$\mathcal{A} \quad \text{hat positive Schnirelman–Dichte.}$$

Nach dem Satz von Schnirelman (1.5) existiert ein $L \in \mathbb{N}$, so dass jedes $n \in \mathbb{N}$ als

$$n = n_1 + \cdots + n_\ell, \quad \ell \le L, \quad n_\nu \text{ prim oder } = 1 \tag{3.1}$$

geschrieben werden kann.

Sei $n \ge 4$. Dann sind in (3.1), angewandt auf $n-2$, vier Fälle möglich

a) alle n_j sind prim,

b) genau ein n_j ist $= 1$,

c) $2a$ $(a \ge 1)$ der n_j sind $= 1$,

d) $2a+1$ $(a \ge 1)$ der n_j sind $= 1$,

Bei a) ist die Behauptung des Satzes wegen $n = n-2+2$ mit $K = L+1$ erfüllt, bei b) wegen $n = n-2+2 = p_1+\cdots+p_{\ell-1}+3$ (etwa $n_\ell = 1$) mit $\le L$ Summanden. Im dritten und vierten Fall werden je zwei oder drei Einsen zu $p = 2$ oder $= 3$ zusammengefasst. Es reichen also stets $\le K = L+1$ prime Summanden.

6. Kapitel. Gleichverteilung

Literatur:

E. Hlawka, Theorie der Gleichverteilung. BI 1979

L. Kuipers, H. Niederreiter, Uniform Distribution of Sequences. Wiley 1974.

Bezeichnungen.

$a, b, c, x, y, z \in \mathbb{Z}$; $d, k, l, m, n, N, q \in \mathbb{N}$; $\alpha, \beta, \gamma \ldots \in \mathbb{R}$;

$e(\alpha) = e^{2\pi i \alpha}$;

$[\alpha] = \max\{a \in \mathbb{Z}, a \le \alpha\}$, Gauß–Klammer,

$\{\alpha\} = \alpha - [\alpha] \in [0, 1)$, gebrochener Anteil von α,

$\|\alpha\| = \min(\alpha - [\alpha], [\alpha] + 1 - \alpha)$, Abstand von α zur nächstgelegenen ganzen Zahl.

Für rationales $\alpha = \dfrac{a}{q}$ durchläuft die Folge $\big(\{n\alpha\}\big)$ nur Werte b/q $\big(b \in \{0, 1, \ldots, q-1\}\big)$, während sie für irrationales α dicht im Einheitsintervall liegt. Dies ist Inhalt des Approximationssatzes von Kronecker (Leopold K., 1823–1891).

6.1. Satz von Kronecker. Sei α irrational. Dann liegt die Menge $\big\{\{n\alpha\}, n \in \mathbb{N}\big\}$ dicht in $[0, 1)$, d.h. zu jedem $\beta \in [0, 1)$ und jedem $\varepsilon > 0$ existieren unendlich viele $n \in \mathbb{N}$, so daß $\big|\{n\alpha\} - \beta\big| < \varepsilon$.

Bem. Daß die Zahlen $\{n\alpha\}$ $(n \in \mathbb{N})$ paarweise verschieden sind, sieht man unmittelbar. Denn wäre für $n_1 < n_2$ $\{n_1\alpha\} = \{n_2\alpha\}$, dann folgte $n_1\alpha - a_1 = n_2\alpha - a_2$,

$$\alpha = \frac{a_2 - a_1}{n_2 - n_1} \in \mathbb{Q}.$$

Zum Beweis von 6.1. wird der folgende, auch sonst vielfach benutzte Hilfssatz benötigt.

6.2. Dirichletscher Approximationssatz.
Sei $\alpha \in \mathbb{R}$, $Q \in \mathbb{N}$, $N \ge 2$. Dann existieren $m \in \mathbb{N}$, $1 \le m \le Q - 1$ und $a \in \mathbb{Z}$ mit $(a, m) = 1$, so dass

$$\Big|\, \alpha - \frac{a}{m} \,\Big| \le \frac{1}{mQ}.$$

Beweis. Die $Q+1$ Zahlen $\{0 \cdot \alpha\}$, $\{\alpha\}, \ldots, \{(Q-q)\alpha\}$ und 1 liegen im Einheitsintervall $[0, 1]$. Darunter muss es zwei geben, die einen Abstand $\le Q^{-1}$ haben (Schubfachschluss!).

Sind dies $\{k_1\alpha\}$ und $\{k_2\alpha\}$ mit $0 \le k_1 < k_2 \le Q - 1$, so gilt mit $m' = k_2 - k_1$ und $a' = [k_1\alpha] - [k_1\alpha]$

$$\big|m'\alpha - a'\big| \le \frac{1}{Q}, \quad \Big|\alpha - \frac{a'}{m'}\Big| \le \frac{1}{m'Q}.$$

Kürzt man a'/m' zu a/m, dann steht dort

$$\left|\alpha - \frac{a}{m}\right| \le \frac{1}{m'Q} \le \frac{1}{mQ}.$$

Sind 1 und $\{k\alpha\}$ solche Zahlen, dann muss $k \neq 0$ sein, und man kommt mit $m' = k$ und $a' = [k\alpha] + 1$ zum Ziel. □

Beweis zu 6.1.
1. Nach 6.2. existiert zu jedem $Q \in \mathbb{N}$ ein $\frac{a}{q} = \frac{a(Q)}{q(Q)} \in \mathbb{Q}$ mit $(a,q) = 1$ und $\delta_Q \underset{\text{Df}}{=} \left|\alpha - \frac{a}{q}\right| \le \frac{1}{qQ} \le \frac{1}{q^2}$.
Wegen $\alpha \notin \mathbb{Q}$ ist stets $\delta_Q \neq 0$, andererseits $\delta_Q \to 0$ für $Q \to \infty$. Die Menge der Nenner $q(Q)$ kann nicht beschränkt sein. Zu jedem $N \in \mathbb{N}$ gibt es also $q \in \mathbb{N}$, $a \in \mathbb{Z}$ mit

$$(1) \qquad q > 2N, \quad (a,q) = 1 \quad \text{und} \quad |q\alpha - a| < q^{-1}.$$

2. Es sei nun $\beta \in [0,1)$ vorgegeben. Werde $c \in \mathbb{Z}$ so bestimmt, daß für das q aus (1) $|q\beta - c\,| \le \frac{1}{2}$ gilt. Wegen $(a,q) = 1$ ist die Gleichung

$$c = ya - xq \quad \text{in} \quad x, y \in \mathbb{Z} \quad \text{mit} \quad |y| \le \frac{1}{2}\, q$$

lösbar. Dann gilt

$$\left|q(y\alpha - x - \beta)\,\right| = \left|\, y(q\alpha - a) + c - q\beta\right| \le \frac{q}{2} \cdot \frac{1}{q} + \frac{1}{2} = 1.$$

Setzt man $n = q + y$, $b = a + x$, dann folgt aus (1) $N < \frac{q}{2} \le n \le \frac{3}{2}\, q$, sowie

$$\left|n\alpha - b - \beta\right| \le \left|y\alpha - x - \beta\right| + \left|q\alpha - a\right| \le \frac{1}{q} + \frac{1}{q} \le \frac{1}{N}.$$

Da dies für jedes N gemacht werden kann, ist der Beweis geführt. □

Der Gedankengang ist erstens schwer zu durchschauen und zweitens gibt er keine Auskunft darüber, inwieweit $\{n\alpha\}$ gleichmäßig im Einheitsintervall verteilt ist. Noch ist zum Beispiel denkbar, daß „wesentlich mehr“ der Zahlen $\{n\alpha\}$ im ersten Halbintervall liegen als im zweiten. Der grundlegende Begriff hierzu ist der der Gleichverteilung einer Folge.

6.3. Def. (Hermann Weyl, 1885–1955, 1916). Eine Folge (α_n) $(n \in \mathbb{N})$ heißt **gleichverteilt** modulo Eins (kurz: gleichverteilt, glv), wenn für alle β und γ mit $0 \le \beta < \gamma \le 1$

$$\lim_{N\to\infty} \frac{1}{N} \#\big\{n \le N, \beta \le \{\alpha_n\} \le \gamma\big\}$$

existiert und gleich $\gamma - \beta$ ist.

Bemerkungen.
1. Es kann oBdA

$$\forall\, n : \alpha_n \in [0,1)$$

vorausgesetzt werden.

2. Es reicht, β und γ mit $0 < \beta < \gamma < 1$ zu betrachten. Denn erfülle für $\alpha_n \in [0,1)$ die Folge (α_n) die Forderung für solche β und γ. Dann gilt für $0 < \varepsilon < \gamma$

$$\lim_{N\to\infty} \frac{1}{N} \#\{n \le N, \varepsilon \le \alpha_n \le \gamma\} = \gamma - \varepsilon,$$

also insbesondere

$$\#\{n \le N, \alpha_n < \varepsilon\} \le 2\varepsilon N \quad \text{für} \quad N \ge N_0(\varepsilon).$$

Sei nun $\beta = 0,\ \ 0 < \gamma < 1$. Dann ergibt sich für $0 < \varepsilon < \gamma$

$$\begin{aligned} &\Big|\frac{1}{N}\ \#\ \{n \le N,\ \alpha_n \le \gamma\} - \gamma\Big| \\ &\le\ \ \frac{1}{N}\#\{n \le N,\ \alpha_n < \varepsilon\} + \Big|\frac{1}{N}\#\{n \le N, \varepsilon \le \alpha_n \le \gamma\} - (\gamma - \varepsilon)\Big| + \varepsilon \\ &\le\ \ 4\varepsilon, \quad \text{falls} \quad N \ge N_0(\gamma, \varepsilon). \end{aligned}$$

Ähnlich geht man im Fall $0 < \beta < \gamma = 1$ vor.

3. Statt $\beta \le \{\alpha_n\} \le \gamma$ kann auch $\beta < \{\alpha_n\} < \gamma$ (bzw. mit gemischten Ungleichungen) gefordert werden. Dies sieht man so wie 2.

Das sogenannte **Weyl–Kriterium** stellt in vielen Fällen die bequemste Methode zum Nachprüfen der Gleichverteilung da.

6.4. Satz. (Weyl, 1916). Die reelle Zahlenfolge (α_n) ist gleichverteilt genau dann, wenn für jedes $h \in \mathbb{N}$

$$\lim_{N\to\infty} \frac{1}{N} \sum_{n\le N} e(h\ \alpha_n) = 0$$

gilt.

Hiermit läßt sich unmittelbar eine Verschärfung des Kroneckerschen Satzes herleiten.

6.5. Satz. Für jedes $\alpha \in \mathbb{R}\backslash\mathbb{Q}$ ist die Folge $(n\alpha)$ gleichverteilt.

Beweis. Mit $\alpha_n = n\alpha$ ergibt sich für $h \in \mathbb{N}$

$$\sum_{n\le N} e(h\ \alpha_n) = \sum_{n=1}^{N} \big(e(h\alpha)\big)^n = e(h\alpha)\ \frac{e(Nh\alpha)-1}{e(h\alpha)-1}.$$

Der Nenner kann wegen $h\alpha \notin \mathbb{Z}$, also $e(h\alpha) \neq 1$, nicht verschwinden. Somit gilt

$$\Big|\frac{1}{N}\ \sum_{n\le N} e(h\ \alpha_n)\Big| \le \frac{2}{N|e(h\alpha)-1|} \to 0 \quad \text{für} \quad N \to \infty.$$

Dies reicht nach dem Weyl–Kriterium für die Gleichverteilung. □

Beweis zum Weylschen Satz.
1. Nach Bemerkung 2. zu 6.3. braucht man zur Herleitung der Gleichverteilung nur β und γ mit $0 < \beta < \gamma < 1$ zu betrachten. $I \underset{\text{Df}}{=} [\beta, \gamma]$. Sei

$$0 < \varepsilon \le \frac{1}{3} \min\ (\beta, 1-\gamma, \gamma-\beta)$$

und für $t \in \mathbb{R}$

$$c_I(t) = \begin{cases} 1, & \text{falls} \quad t \in I \\ 0 & \text{sonst} \end{cases}$$

(Indikatorfunktion zum Intervall I).
c_I werde von unten und oben approximiert durch auf $[0,1]$ zweimal stetig differenzierbare Funktionen f_u und f_0.

$$f_u(t) = \begin{cases} 0, & \text{falls} \quad 0 \le t \le \beta & \text{oder} \quad \gamma \le t \le 1, \\ \in [0,1], & \text{falls} \quad \beta \le t \le \beta+\varepsilon & \text{oder} \quad \gamma-\varepsilon \le t \le \gamma, \\ 1, & \text{falls} \quad t \in [\beta+\varepsilon, \gamma-\varepsilon]. \end{cases}$$

$$f_o(t) = \begin{cases} 0, & \text{falls} \quad 0 \le t \le \beta-\varepsilon \quad \text{oder} \quad \gamma+\varepsilon \le t \le 1, \\ \in [0,1], & \text{falls} \quad \beta-\varepsilon \le t \le \beta \quad \text{oder} \quad \gamma \le t \le \gamma+\varepsilon, \\ 1, & \text{falls} \quad \beta \le t \le \gamma. \end{cases}$$

Auf das genaue Aussehen von f_u und f_o kommt es nicht an. Offenbar gilt

$$f_u \le c_I \le f_o. \tag{1.1}$$

$f_u < f_o$ nur in Punkten der Intervalle $(\beta-\varepsilon, \beta+\varepsilon)$ und $(\gamma-\varepsilon, \gamma+\varepsilon)$.

2. Sei $\alpha_n \in [0,1)$ für alle n. Wegen

$$\#\big\{n \le N, \alpha_n \in [\beta,\gamma]\big\} = \sum_{n\le N} c_I(\alpha_n)$$

reicht es für die Gleichverteilung zu zeigen

$$\Big|\sum_{n\le N} c_I(\alpha_n) - N(\gamma-\beta)\Big| \le 4\varepsilon N, \quad \text{falls} \quad N \ge N_0(\varepsilon,\beta,\gamma). \tag{2.1}$$

3. f_u und f_o sind Fourier–entwickelbar

$$f_u(t) = \sum_{a\in\mathbb{Z}} \eta_a\ e(at), \qquad f_o(t) = \sum_{a\in\mathbb{Z}} \rho_a\ e(at) \tag{3.1}$$

mit

$$\eta_a = \int_0^1 f_u(t)\ e(-at)\ dt, \qquad \eta_0 = \int_0^1 f_u(t)\ dt, \quad \big|\eta_0 - (\gamma-\beta)\big| \le 2\varepsilon. \tag{3.2}$$

Ebenso die ρ_a. Für $a \neq 0$ ist wegen

$$\begin{aligned} f_u(0) = f_u'(0) = f_u(1) = f_u'(1) &= 0 \\ \eta_a = \int_0^1 f_u(t)\ \frac{d}{dt}\Big(\frac{e(-at)}{-2\pi i a}\Big)dt &= \frac{1}{2\pi i a}\int_0^1 f_u'(t)\ e(-at)\ dt \\ = \frac{1}{(2\pi i a)^2}\int_0^1 f_u''(t)\ e(-at)\ dt. & \end{aligned}$$

Mit

$$M \underset{\text{Df}}{=} \max\ \big(\max_{0\le t\le 1}\big|f_u''(t)\big|,\ \max_{0\le t\le 1}\big|f_o''(t)\big|\big) \tag{3.3}$$

folgt hieraus (für ρ_a analog)

$$|\eta_a|,\ |\rho_a| \le \frac{M}{4\pi^2 a^2}\ , \quad a \neq 0. \tag{3.4}$$

Insbesondere existiert ein $A_0 \in \mathbb{N}$ mit

$$\sum_{a\in\mathbb{Z},|a|>A_0} \big(|\eta_a| + |\rho_a|\big) < \varepsilon. \tag{3.5}$$

4. Zum Beweis der Richtung von rechts nach links werde die Konvergenzbedingung für die Exponentialsummen vorausgesetzt. Insbesondere existiert ein $N_0 \in \mathbb{N}$ mit

$$\forall\ N \ge N_0\ \forall\ a \in \mathbb{Z}\backslash\{0\}:\ |a| \le A_0 \Rightarrow \Big|\sum_{n\le N} e(a\ \alpha_n)\Big| \le \frac{N\varepsilon}{A_0 M}\ . \tag{4.1}$$

Mit (3.1), (3.2), (3.5) und (4.1) erhält man für $N \geq N_0$

$$\begin{aligned}
&\Big|\sum_{n\leq N} f_u(\alpha_n) - N(\gamma-\beta)\Big| \\
&\leq \big|\eta_0 - (\gamma-\beta)\big|\ N + \sum_{0<|a|\leq A_0} |\eta_a|\ \Big|\sum_{n\leq N} e(a\ \alpha_n)\Big| + \sum_{|a|>a_0} |\eta_a| N \\
&\leq 2\varepsilon N + \sum_{0<|a|\leq A_0} \frac{M}{4\pi^2 a^2}\ N\ \frac{\varepsilon}{A_0 M} + \varepsilon N \\
&\leq 4\varepsilon N.
\end{aligned}$$

Ebenso für f_o. Mit (1.1) ergibt sich daraus (2.1). Damit ist die eine Richtung gezeigt.

5.1. Es werde die Gleichverteilung von (α_n) vorausgesetzt. Sei $0 < \varepsilon < 1$ und $a \in \mathbb{N}$. Es werde k so groß gewählt, daß

$$\frac{4\pi a}{k} < \frac{\varepsilon}{2} \tag{5.1.1}$$

gilt. Für $1 \leq \nu \leq k$ sei

$$I_\nu = I_{\nu,k} = \Big[\frac{\nu-1}{k}, \frac{\nu}{k}\Big).$$

Die Voraussetzung ergibt

$$\frac{1}{N}\#\{n \leq N, \alpha_n \in I_\nu\} \to 1/k \quad \text{für} \quad N \to \infty.$$

Insbesondere existiert ein $N_0 = N_0(\varepsilon, a)$, so dass für alle $N \geq N_0$ und alle $\nu \leq k$

$$\begin{aligned}
\Big|\#\{n \leq N, \alpha_n \in I_\nu\} - \frac{N}{k}\Big| &< \frac{N\varepsilon}{2k} \quad \text{und} \\
\#\{n \leq N, \alpha_n \in I_\nu\} &< \frac{2N}{k}
\end{aligned} \tag{5.1.2}$$

erfüllt ist.

5.2. Für $\beta, \gamma \in \mathbb{R}$ ist

$$\begin{aligned}
\big|e(\beta) - e(\gamma)\big| &= \big|1 - e(\gamma-\beta)\big| \\
&= \Big|\int_0^{\gamma-\beta} 2\pi i\ e(t)\ dt\Big| \leq 2\pi\big|\gamma-\beta\big|.
\end{aligned}$$

5.3. Sei $N \geq N_0$. Man sieht unmittelbar

$$\begin{aligned}\sum_{n\leq N} e(a\ \alpha_n) &= \sum_{\nu=1}^{k} \sum_{n\leq N,\alpha_n\in I_\nu} e(a\ \alpha_n)\\ &= \sum_{\nu=1}^{k} e\Big(a\frac{\nu}{k}\Big)\#\{n\leq N,\alpha_n\in I_\nu\}\\ &+ \sum_{\nu=1}^{k} \sum_{n\leq N,\alpha_n\in I_\nu} \Big(e(a\ \alpha_n) - e\Big(a\frac{\nu}{k}\Big)\Big).\end{aligned}$$

Mit (5.1.1), (5.1.2), 5.2. und der Beziehung $\sum_{\nu=1}^{k} e\Big(a\frac{\nu}{k}\Big) = 0$ (da nach (5.1.1) $a < k$) ergibt sich daraus

$$\begin{aligned}\Big|\sum_{n\leq N} e(a\ \alpha_n)\Big| &\leq 2\frac{N}{k}\ \Big|\sum_{\nu=1}^{k} e\Big(a\frac{\nu}{k}\Big)\Big| + \sum_{\nu=1}^{k}\Big|\#\{n\leq N,\alpha_n\in I_\nu\} - \frac{N}{k}\Big|\\ &\quad + \sum_{\nu=1}^{k}\#\{n\leq N,\alpha_n\in I_\nu\}\cdot 2\pi\frac{a}{k}\\ &\leq 0 + k\cdot\frac{N\varepsilon}{2k} + k\cdot\frac{2N}{k}\cdot 2\pi\frac{a}{k} < \varepsilon N.\end{aligned}$$

Damit ist auch die andere Richtung bewiesen. □

Die Definition der Gleichverteilung und das Weyl–Kriterium können ohne weiteres ins Mehrdimensionale übertragen werden.

6.6. Def. Eine Folge $(\alpha_n) = \big((\alpha_{n1},\ldots,\alpha_{nk})\big)$ aus $\mathbb{R}^k$ heißt **gleichverteilt**, wenn für jedes k–dimensionale Intervall

$$I = [\beta_1,\gamma_1]\times\ldots\times[\beta_k,\gamma_k]\subseteq[0,1]^k$$

gilt

$$\lim_{N\to\infty}\frac{1}{N}\,\#\{n\leq N,\alpha_n\in I\} = (\gamma_1-\beta_1)\ldots(\gamma_k-\beta_k).$$

6.7. Satz. (Weyl–Kriterium im k–Dimensionalen).
Eine Folge (α_n) aus $\mathbb{R}^k$ ist gleichverteilt genau dann, wenn für jedes $a = (a_1,\ldots,a_k)\in\mathbb{Z}^k\backslash(0,\ldots,0)$ gilt

$$\lim_{N\to\infty}\frac{1}{N}\sum_{n\leq N} e\big(a_1\alpha_{n1}+\ldots+a_k\alpha_{nk}\big) = 0.$$

Mit 6.7. kann der allgemeine Kroneckersche Approximationssatz eingesehen werden.

6.8. Satz. Seien $1, \alpha_1, \ldots, \alpha_k$ linear unabhängig über $\mathbb{Q}$. Dann ist die Folge $\big((n\alpha_1, \ldots, n\alpha_k)\big)$ gleichverteilt. Insbesondere liegen die Punkte $(n\alpha_1, \ldots, n\alpha_k)$ $(n \in \mathbb{N})$ dicht in $[0,1]^k$

Denn sei $(a_1, \ldots, a_k) \neq (0, \ldots, 0)$, oBdA $a_1, \ldots, a_j \neq 0$, $a_{j+1} = \ldots = a_k = 0$ für ein j mit $1 \leq j \leq k$. Dann ergibt sich

$$\sum_{n \leq N} e(a_1\alpha_{n1} + \ldots + a_k\alpha_{nk}) = \sum_{n \leq N} e\big(n(a_1\alpha_1 + \ldots + a_j\alpha_j)\big).$$

Wegen der linearen Unabhängigkeit ist $a_1\alpha_1 + \ldots + a_j\alpha_j$ irrational, und man verfährt wie bei $k = 1$. □

Satz 6.5. besagt, daß die Werte $f(n)$ der Funktion $f(x) = \alpha x$ $(\alpha \in \mathbb{R}\backslash\mathbb{Q})$ gleichverteilt sind. In seiner grundlegenden Arbeit von 1916 untersuchte Hermann Weyl Folgen von Polynomwerten.

6.9. Satz (Weyl, 1916). Sei

$$f(x) = \beta_k\, x^k + \ldots + \beta_0 \quad (\beta_0, \ldots, \beta_k \in \mathbb{R}, k \geq 1),$$

wobei mindestens eine der Zahlen $\beta_1, \ldots, \beta_k$ irrational ist. Dann ist die Folge $\big(f(n)\big)$ $(n \in \mathbb{N})$ gleichverteilt.

Der Beweis soll hier in kürzerer Form nach van der Corput (Johannes v.d. C., 1890 – 1975) geführt werden.

6.10. Hilfssatz (van der Corput, 1926). Für komplexe Zahlen $w_1, \ldots, w_N$ und $H \in \mathbb{N}$ mit $1 \leq H \leq N$ besteht die Ungleichung

$$H^2\Big|\sum_{n=1}^{N} w_n\Big|^2 \leq H(N+H-1)\sum_{n=1}^{N}|w_n|^2 + 2(H+N-1)\sum_{h=1}^{H-1}(H-h)\mathrm{Re}\sum_{n=1}^{N-h} w_n\,\overline{w}_{n+h}.$$

Beweis. Es werde $w_n = 0$ gesetzt für $n \leq 0$ bzw. $n > N$. Durch Auszählen sieht man leicht

$$H\sum_{n=1}^{N} w_n = \sum_{k=1}^{N+H-1}\ \sum_{m=0}^{H-1} w_{k-m}. \tag{1}$$

Anwendung der Cauchy–Schwarz–Ungleichung ergibt

$$\begin{aligned} H^2\Big|\sum_{n=1}^{N} w_n\Big|^2 &\le (N+H-1)\sum_{k=1}^{N+H-1}\Big|\sum_{m=0}^{H-1} w_{k-m}\Big|^2 \\ &= (H+N-1)\sum_{k=1}^{N+H-1}\sum_{m=0}^{H-1} w_{k-m}\sum_{\ell=0}^{H-1}\overline{w}_{k-\ell} \\ &= (H+N-1)\sum_{k=1}^{N+H-1}\sum_{m=0}^{H-1}\big|w_{k-m}\big|^2 \\ &\quad + 2(H+N-1)\mathrm{Re}\sum_{k=1}^{N+H-1}\sum_{\substack{m,\ell=0\\ \ell<m}}^{H-1} w_{k-m}\,\overline{w}_{k-\ell}. \end{aligned} \tag{2}$$

Die beiden Doppelsummen seien mit $\sum_1$ bzw. $\sum_2$ bezeichnet. $\sum_1$ erweist sich wie in (1) als

$$H\sum_{n=1}^{N}\big|w_n\big|^2. \tag{3}$$

In $\sum_2$ werde $k-m$ in n $(1\le n\le N)$ und $k-\ell$ in $n+h$ $(1\le h\le H-1)$ umbenannt. Für festes n und h tritt $w_n\,\overline{w}_{n+h}$ in $\sum_2$ genau $(H-h)-$mal auf, nämlich mit den Indizes

$$\begin{aligned} (k-m,k-\ell) =& \big((n+h)-h,(n+h)-0\big),\big(n+(h+1)-(h+1),n+(h+1)-1\big),\dots, \\ & \big(n+(H-1)-(H-1),n+(H-1)-(H-h-1)\big). \end{aligned}$$

Dies führt zu

$$\begin{aligned} \sum\nolimits_2 &= \sum_{h=1}^{H-1}(H-h)\sum_{n=1}^{N} w_n\,\overline{w}_{n+h} \\ &= \sum_{h=1}^{H-1}(H-h)\sum_{n=1}^{N-h} w_n\,\overline{w}_{n+h}. \end{aligned}$$

Zusammenfassung ergibt die Behauptung. □

6.11. Van der Corputscher Differenzensatz.
Sei (α_n) eine Folge aus $\mathbb{R}$ mit der Eigenschaft, daß für jedes $h\in\mathbb{N}$ die Differenzenfolge $(\alpha_{n+h}-\alpha_n)$ gleichverteilt ist. Dann ist (α_n) gleichverteilt.

Beweis. Für $a\in\mathbb{N}$ wird 6.10. auf die Zahlen $w_n=e(a\,\alpha_n)$ angewandt. Für $\varepsilon>0$ sei

$H \in \mathbb{N}$ mit $H^{-1} < \varepsilon$ fest gewählt. Dann folgt für $N > H$

$$\Big|\frac{1}{N}\sum_{n\le N} e(a\ \alpha_n)\Big|^2$$
$$\le \frac{N+H-1}{HN} + 2\sum_{h=1}^{H-1} \frac{(N+H-1)(H-h)(N-h)}{H^2N^2}\cdot\frac{1}{N-h}\cdot\Big|\sum_{n=1}^{N-h} e\big(a(\alpha_n-\alpha_{n+h})\big)\Big|.$$

Für $N \ge N_0(\varepsilon)$ ist nach Voraussetzung und dem Weyl–Kriterium jeder der Beträge rechts $\le (N-h)\varepsilon$. Damit wird

$$\Big|\frac{1}{N}\sum_{n\le N} e(a\ \alpha_n)\Big|^2 \le \frac{2}{H} + 4\varepsilon \le 6\varepsilon,$$

was nach dem Weyl–Kriterium der Behauptung entspricht. □

Beweis zu Satz 6.9.

1. Sei $1 \le g \le k$ der größte Index mit irrationalem Koeffizienten β_g. Der Beweis wird durch Induktion nach g geführt.

2. Im Fall $g = 1$ kann $k \ge 2$ vorausgesetzt werden, da

$$f(x) = \beta_1 x + \beta_0, \qquad \beta_1 \in \mathbb{R}\backslash\mathbb{Q}$$

direkt mit dem Weyl–Kriterium behandelt werden kann. Sei also

$$f(x) = F(x) + \beta_1 x + \beta_0 \quad \beta_1 \in \mathbb{R}\backslash\mathbb{Q},$$
$$F(x) = \beta_2 x^2 + \ldots + \beta_k x^k \quad \text{mit} \quad \beta_2, \ldots, \beta_k \in \mathbb{Q}.$$

Bezeichne D das kgV der Nenner von $\beta_2, \ldots, \beta_k$. Dann gilt für $1 \le r \le D,\ m \in \mathbb{N}$ und $a \in \mathbb{N}$

$$\{af(mD+r)\} = \{aF(r) + a\beta_1(mD+r) + a\beta_0\}$$

und somit

$$\sum_{n=1}^{N} e\big(af(n)\big) = \sum_{r=1}^{D}\sum_{m=0}^{[N/D]-1} e\big(aF(r) + a\beta_1(mD+r) + a\beta_0\big) + \sum_{n=D[N/D]+1}^{N} e\big(af(n)\big),$$

$$\Big|\frac{1}{N}\sum_{n\le N} e\big(af(n)\big)\Big| \le \frac{1}{N}\sum_{r=1}^{D}\Big|\sum_{m=0}^{[N/D]-1} e(amD\beta_1)\Big| + \frac{D}{N}.$$

Jede der D m–Summen kann wegen $D\beta_1 \notin \mathbb{Q}$ hinreichend gut abgeschätzt werden. Mit dem Weyl–Kriterium folgt die Behauptung in diesem Fall $(g = 1)$.

3. Sei nun $g \geq 2$ und die Behauptung für alle Polynome mit dem Index $g-1$ schon bewiesen. Für festes $h \in \mathbb{N}$ bilde man im Hinblick auf 6.11. das Differenz–Polynom

$$\begin{aligned} f_h(x) &= f(x+h) - f(x) \\ &= \beta_k\big((x+h)^k - x^k\big) + \ldots + \beta_g\big((x+h)^g - x^g\big) + \ldots + \beta_1\, h \\ &= \gamma_{k-1}x^{k-1} + \ldots + \gamma_{g-1}x^{g-1} + \ldots + \gamma_0 \end{aligned}$$

mit von h abhängenden $\gamma_0, \ldots, \gamma_{k-1}$. Man überzeugt sich leicht, daß $\gamma_g, \ldots, \gamma_{k-1} \in \mathbb{Q}$, aber $\gamma_{g-1} \in \mathbb{R}\backslash\mathbb{Q}$. Damit ist die Induktionsvoraussetzung auf f_h anwendbar. Mit 6.11. ergibt sich die Behauptung. □

Hier wurde, vergleichbar zum Beweis des Linnikschen Hilfssatzes in Kap. 1, das Problem durch mehrfache Differenzbildung auf den linearen Fall zurückgeführt. Bei wesentlich schneller wachsenden Folgen versagt diese Idee. So ist bis heute ungeklärt, ob die Folge $\big(\exp(n)\big)$ gleichverteilt ist.

Ähnlich wie bei der Konvergenz einer Folge (langsame oder rasche) gibt es Unterschiede in der Güte der Gleichverteilung. Ein Maß hierfür ist die sog. Diskrepanz einer Folge.

6.12. Def. Sei $N \in \mathbb{N},\ \alpha_1, \ldots, \alpha_N \in [0,1)$.

$$D_N = D_N(\alpha) \underset{\text{Df}}{=} \sup_{\beta,\gamma,0\leq\beta\leq\gamma\leq 1} \Big|\frac{1}{N}\#\{n \leq N, \alpha_n \in [\beta,\gamma]\} - (\gamma-\beta)\Big|$$

heißt die **Diskrepanz** (der endlichen Folge $\alpha_1, \ldots, \alpha_N$).

Bemerkungen.
1. Stets gilt

$$N^{-1} \leq D_N \leq 1.$$

Zur unteren Schranke: Zu jedem $\varepsilon > 0$ läßt sich ein Intervall $[\beta,\gamma]$ mit $\gamma - \beta > N^{-1} - \varepsilon$ finden, in dem kein α_j liegt.

2. Es reicht, β und γ mit $0 < \beta < \gamma < 1$ zu betrachten.

3. Eine Folge (α_n) aus $[0,1)$ ist gleichverteilt genau dann, wenn

$$\lim_{N\to\infty} D_N(\alpha_1, \ldots, \alpha_N) = 0.$$

Aus der Bedingung an D_N folgt unmittelbar die Gleichverteilung.

Zur umgekehrten Richtung sei $\varepsilon > 0$ und $k^{-1} < \varepsilon$. Für jedes Teilintervall I^* eines Intervalls $\left[\frac{\nu}{k}, \frac{\nu+1}{k}\right)$ $(0 \le \nu \le k-1)$ gilt nach der Gleichverteilung für $N \ge N_0(\varepsilon, k)$

$$\frac{1}{N} \# \{n \le N,\ \alpha_n \in I\} \le \frac{2}{k} < 2\varepsilon.$$

Für beliebige β, γ mit $0 \le \beta < \gamma \le 1$ läßt sich $[\beta, \gamma]$ schreiben als disjunkte Vereinigung von (evtl. leeren) Intervallen I_1^*, $\left[\frac{\nu}{k}, \frac{\mu+1}{k}\right)$, I_2^* mit $0 \le \nu \le \mu \le k-1$, I_1^* und I_2^* wie das obige I^*, also $\left|\gamma - \beta - \frac{\mu+1-\nu}{k}\right| \le \frac{2}{k}$.

Erneut folgt aus der Gleichverteilung für $N \ge N_0$ und alle ν, μ

$$\left| \# \left\{n \le N, \frac{\nu}{k} \le \alpha_n \le \frac{\mu+1}{k}\right\} - \frac{\mu+1-\nu}{k}\right| \le \varepsilon N.$$

Hieraus ergibt sich für $N \ge N_0$

$$\begin{aligned}
&\left|\frac{1}{N} \# \{n \le N, \beta \le \alpha_n \le \gamma\} - (\gamma - \beta)\right| \\
&\le \left|\frac{1}{N} \# \{n \le N, \beta \le \alpha_n \le \gamma\} - \frac{1}{N} \# \left\{n \le N, \frac{\nu}{k} \le \alpha_n \le \frac{\mu+1}{k}\right\}\right| \\
&\quad + \left|\frac{1}{N} \# \left\{n \le N, \frac{\nu}{k} \le \alpha_n \le \frac{\mu+1}{k}\right\} - \frac{\mu+1-\nu}{k}\right| + \left|\frac{\mu+1-\nu}{k} - (\gamma - \beta)\right| \\
&\le 4\varepsilon + \varepsilon + \frac{2}{k} < 7\varepsilon.
\end{aligned}$$

Wegen der Gleichmäßigkeit in β und γ ist dies dasselbe wie $D_N \to 0$. □

Eine Art quantitativer Version des Weylschen Kriteriums ist die
Ungleichung von Erdös–Turán (Paul E., 1913–1996; Paul T., 1910–1976; 1948)
Für beliebige $\alpha_1, \ldots, \alpha_N \in [0, 1)$ gilt

$$D_N \le \frac{6}{m+1} + \frac{4}{\pi} \sum_{h=1}^{m} \left(\frac{1}{h} - \frac{1}{m+1}\right) \left|\frac{1}{N} \sum_{n \le N} e\big(h\ \alpha_n\big)\right|.$$

Dabei ist m eine frei zu wählende natürliche Zahl $\le N$.

Der Beweis verläuft ähnlich wie beim Weyl–Kriterium über Fourier–Reihen.

Es ist leicht, hiermit die eine Richtung des Weyl–Kriteriums zu beweisen.

Es erhebt sich die Frage, ob die untere Grenze N^{-1} in Bemerkung 1. wirklich durch spezielle Folgen, erstklassig gleichverteilte, stets erreicht wird. Dass dies nicht sein kann,

zeigte 1945 die niederländische Mathematikerin Tatiana **van Aardenne–Ehrenfest:** es existiert ein $C > 0$, so daß für jede Folge (α_n) aus $[0,1)$ und unendlich viele N die Ungleichung

$$D_N(\alpha) \geq C\ N^{-1} \ln\ln\ln N \tag{AE}$$

gilt.
Das beste diesbezügliche Ergebnis wurde 1972 von **Wolfgang Schmidt** gezeigt. Die Ungleichung (AE) kann zu

$$D_N(\alpha) \geq C\ N^{-1} \ln N \tag{S}$$

verschärft werden. Der Beweis ist elementar, aber sehr raffiniert.

Umgekehrt gibt es Folgen (α_n), für die stets

$$D_N(\alpha) = \mathrm{O}(N^{-1} \ln N)$$

gilt, zum Beispiel $\alpha_n = n\alpha$ für geeignete $\alpha \in \mathbb{R}\backslash\mathbb{Q}$. Besonders gut zugänglich ist eine 1935 von van der Corput angegebene Folge.

6.13. Satz. Sei

$$\begin{aligned} n &= a_\ell\ 2^\ell + a_{\ell-1}\ 2^{\ell-1} + \ldots + a_1 \cdot 2 + a_0 \quad \big(a_0, \ldots, a_\ell \in \{0,1\},\ a_\ell = 1\big). \\ \alpha_n &= a_0 \cdot 2^{-1} + a_1 \cdot 2^{-2} + \ldots + a_\ell \cdot 2^{-\ell-1} \end{aligned}$$

(**van der Corput–Folge**).
Dann gilt für $N > 1$

$$D_N(\alpha) = \mathrm{O}\big(N^{-1} \ln N\big).$$

Beweis. 1. Sei $N > 1,\ 2^r \leq N$ und $0 \leq k < 2^r$. Es sollen die $n \leq N$ mit

$$\alpha_n \in \big[k\ 2^{-r}, (k+1)\ 2^{-r}\big) \tag{1.1}$$

gezählt werden. Sei

$$k\ 2^{-r} = b_0\ 2^{-1} + \ldots + b_{r-1}\ 2^{-r}.$$

Dann bedeutet (1.1)

$$\alpha_n = b_0\ 2^{-1} + \ldots + b_{r-1}\ 2^{-r} + c_r\ 2^{-r-1} + \ldots$$

mit beliebigen $c_r, c_{r+1}, \ldots$ Für n bedeutet dies, daß es die Anfangsziffern $b_0, \ldots, b_{r-1}$ hat, bzw.

$$n \equiv b_0 + b_1 \cdot 2 + \ldots + b_{r-1}\ 2^{r-1} \qquad (2^r).$$

Dies sind die Zahlen in genau einer durch k festgelegten Restklasse mod 2^r. Unterhalb N sind dies mindestens $[N2^{-r}]$ und höchstens $[N2^{-r}+1]$ Zahlen. Damit ergibt sich

$$\left|N^{-1}\#\{n \le N, k\ 2^{-r} \le \alpha_n < (k+1)\ 2^{-r}\} - 2^{-r}\right| \le N^{-1}. \tag{1.2}$$

2. Sei $R \in \mathbb{N}$ mit $2^R \le N$ (es wird am Ende geeignet gewählt). Für beliebige β und γ mit $0 \le \beta < \gamma \le 1$ soll das Intervall $[\beta, \gamma]$ von innen her durch paarweise disjunkte Intervalle

$$\left[k\ 2^{-r}, (k+1)\ 2^{-r}\right) \qquad (1 \le r \le R, \quad 0 \le k < 2^r)$$

ausgeschöpft werden.

2.1. Im ersten Schritt wähle man – falls es überhaupt möglich ist – $r_1 \le R$ minimal, so daß ein Intervall $I_{11} = \left[k_1\ 2^{-r_1}, (k_1+1)\ 2^{-r_1}\right)$ bzw. zwei aneinandergrenzende solche Intervalle I_{11}, I_{12} ganz in $[\beta, \gamma]$ liegen (z.B.) $I_{11} = \left[\frac{2}{4}, \frac{3}{4}\right)$ bei $[\beta, \gamma] = \left[\frac{1}{2} - \frac{1}{10}, \frac{3}{4} + \frac{1}{10}\right]$, aber $I_{11} = \left[\frac{1}{4}, \frac{2}{4}\right), I_{12} = \left[\frac{2}{4}, \frac{3}{4}\right)$ bei $[\beta, \gamma] = \left[\frac{1}{4} - \frac{1}{10}, \frac{3}{4} + \frac{1}{10}\right]\Big)$.
Es bleiben höchstens zwei Randstücke der Länge $< 2^{-r_1}$.

2.2. Mit den Randstücken fährt man so fort und erhält maximal vier Intervalle $I_{21}, I_{22}, \ldots$ zu Indizes r_2, r_2' mit $r_1 < r_2, r_2' \le R$.

2.3. Das Verfahren wird fortgesetzt, bis keine Intervalle mit Index $\le R$ mehr eingefügt werden können. Man erhält so insgesamt $K \le 4R$ Intervalle $J_1, \ldots, J_K$ von der in 1. betrachteten Form. Bezeichne $\mu(J)$ die Länge eines Intervalls J. Dann gilt

$$\left|(\gamma - \beta) - \sum_{\nu=1}^{K} \mu(J_\nu)\right| \le 2 \cdot 2^{-R}. \tag{2.3}$$

Durch Hinzufügen von jeweils einem Intervall zum Index 2^{-R} links und rechts an $\bigcup J_\nu$ erreicht man eine Obermenge von $[\beta, \gamma]$.

3. Es ist

$$\begin{aligned}
&\left|N^{-1}\#\{n \le N, \alpha_n \in [\beta, \gamma]\} - (\gamma - \beta)\right| \\
&\quad \le \left|N^{-1}\#\{n \le N, \alpha_n \in [\beta, \gamma]\} - \sum_{\nu=1}^{K} N^{-1}\#\{n \le N, \alpha_n \in J_\nu\}\right| \\
&\qquad + \sum_{\nu=1}^{K} \left|N^{-1}\#\{n \le N, \alpha_n \in J_\nu\} - \mu(J_\nu)\right| + \left|\sum_{\nu=1}^{K} \mu(J_\nu) - (\gamma - \beta)\right|.
\end{aligned}$$

Die erste Differenz rechts ist nach 2.1. und (1.2) $\leq 2 \cdot 2^{-R} + 2N^{-1}$, die zweite wegen $K \leq 4R$ und (1.2) $\leq 4R\ N^{-1}$, die dritte nach (2.3) $\leq 2 \cdot 2^{-R}$. Also folgt

$$\big|N^{-1}\#\big\{n \leq N, \alpha_n \in [\beta,\gamma]\big\} - (\gamma - \beta)\big| \leq 8(2^{-R} + R\ N^{-1}). \tag{3.1}$$

Wählt man $R = [\ln N / \ln 2]$, dann wird die rechte Seite in (3.1) $\leq c\ N^{-1} \ln N$ mit einem universellen c. Damit ist die Behauptung bewiesen. □